Guida di riferimento

AWS Policy gestita

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Policy gestita: Guida di riferimento

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Cosa sono le policy AWS gestite? 1
Comprendere le pagine di riferimento delle politiche 1
Policy gestite obsolete AWS 2
AWS policy gestite 3
AccessAnalyzerServiceRolePolicy 55
Utilizzo di questa politica 55
Dettagli della policy 55
Versione della politica 55
Documento di policy JSON 56
Ulteriori informazioni 58
AccountAccessManagerServiceRolePolicy 58
Utilizzo di questa politica 59
Dettagli della policy 59
Versione della politica 59
Documento di policy JSON 59
Ulteriori informazioni 60
AccountManagementFromVercel 60
Utilizzo di questa politica 60
Dettagli della policy 60
Versione della politica 60
Documento di policy JSON 61
Ulteriori informazioni 62
AdministratorAccess 62
Utilizzo di questa politica 63
Dettagli della policy 63
Versione della politica 63
Documento sulla politica JSON 63
Ulteriori informazioni 63
AdministratorAccess-Amplify 64
Utilizzo di questa politica 64
Dettagli della policy 64
Versione della politica 64
Documento di policy JSON 64
Ulteriori informazioni 75

AdministratorAccess-AWSElasticBeanstalk 75
Utilizzo di questa politica 75
Dettagli della policy 75
Versione della politica 75
Documento di policy JSON 76
Ulteriori informazioni 84
AIDevOpsAgentAccessPolicy 84
Utilizzo di questa politica 84
Dettagli della policy 84
Versione della politica 85
Documento di policy JSON 85
Ulteriori informazioni 106
AIDevOpsAgentActionsPolicy 106
Utilizzo di questa politica 106
Dettagli della policy 106
Versione della politica 107
Documento di policy JSON 107
Ulteriori informazioni 107
AIDevOpsAgentFullAccess 108
Utilizzo di questa politica 108
Dettagli della policy 108
Versione della politica 108
Documento di policy JSON 108
Ulteriori informazioni 111
AIDevOpsAgentReadOnlyAccess 111
Utilizzo di questa politica 111
Dettagli della policy 111
Versione della politica 111
Documento di policy JSON 111
Ulteriori informazioni 112
AIDevOpsOperatorAppAccessPolicy 112
Utilizzo di questa politica 112
Dettagli della policy 112
Versione della politica 113
Documento di policy JSON 113
Ulteriori informazioni 116

AIOpsAssistantIncidentReportPolicy 116
Utilizzo di questa politica 116
Dettagli della policy 116
Versione della politica 116
Documento di policy JSON 117
Ulteriori informazioni 117
AIOpsAssistantPolicy 118
Utilizzo di questa politica 118
Dettagli della policy 118
Versione della politica 118
Documento di policy JSON 118
Ulteriori informazioni 139
AIOpsConsoleAdminPolicy 139
Utilizzo di questa politica 139
Dettagli della policy 140
Versione della politica 140
Documento di policy JSON 140
Ulteriori informazioni 146
AIOpsOperatorAccess 146
Utilizzo di questa politica 146
Dettagli della policy 146
Versione della politica 147
Documento di policy JSON 147
Ulteriori informazioni 150
AIOpsReadOnlyAccess 150
Utilizzo di questa politica 150
Dettagli della policy 150
Versione della politica 150
Documento di policy JSON 151
Ulteriori informazioni 151
AlexaForBusinessDeviceSetup 151
Utilizzo di questa politica 152
Dettagli della policy 152
Versione della politica 152
Documento di policy JSON 152
Ulteriori informazioni 153

AlexaForBusinessFullAccess 153
Utilizzo di questa politica 153
Dettagli della policy 153
Versione della politica 153
Documento di policy JSON 154
Ulteriori informazioni 155
AlexaForBusinessGatewayExecution 155
Utilizzo di questa politica 155
Dettagli della policy 155
Versione della politica 156
Documento di policy JSON 156
Ulteriori informazioni 157
AlexaForBusinessLifesizeDelegatedAccessPolicy 157
Utilizzo di questa politica 157
Dettagli della policy 157
Versione della politica 157
Documento di policy JSON 158
Ulteriori informazioni 160
AlexaForBusinessNetworkProfileServicePolicy 160
Utilizzo di questa politica 160
Dettagli della policy 160
Versione della politica 161
Documento di policy JSON 161
Ulteriori informazioni 162
AlexaForBusinessPolyDelegatedAccessPolicy 162
Utilizzo di questa politica 162
Dettagli della policy 162
Versione della politica 162
Documento di policy JSON 162
Ulteriori informazioni 164
AlexaForBusinessReadOnlyAccess 164
Utilizzo di questa politica 164
Dettagli della policy 165
Versione della politica 165
Documento di policy JSON 165
Ulteriori informazioni 165

AmazonAPIGatewayAdministrator 166
Utilizzo di questa politica 166
Dettagli della policy 166
Versione della politica 166
Documento di policy JSON 166
Ulteriori informazioni 167
AmazonAPIGatewayInvokeFullAccess 167
Utilizzo di questa politica 167
Dettagli della policy 167
Versione della politica 167
Documento di policy JSON 168
Ulteriori informazioni 168
AmazonAPIGatewayPushToCloudWatchLogs 168
Utilizzo di questa politica 168
Dettagli della policy 168
Versione della politica 169
Documento di policy JSON 169
Ulteriori informazioni 169
AmazonAppFlowFullAccess 170
Utilizzo di questa politica 170
Dettagli della policy 170
Versione della politica 170
Documento di policy JSON 170
Ulteriori informazioni 173
AmazonAppFlowReadOnlyAccess 173
Utilizzo di questa politica 173
Dettagli della policy 173
Versione della politica 174
Documento di policy JSON 174
Ulteriori informazioni 174
AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy 175
Utilizzo di questa politica 175
Dettagli della policy 175
Versione della politica 175
Documento di policy JSON 175
Ulteriori informazioni 176

AmazonAppStreamFullAccess 176
Utilizzo di questa politica 177
Dettagli della policy 177
Versione della politica 177
Documento di policy JSON 177
Ulteriori informazioni 179
AmazonAppStreamPCAAccess 179
Utilizzo di questa politica 179
Dettagli della policy 179
Versione della politica 180
Documento di policy JSON 180
Ulteriori informazioni 180
AmazonAppStreamReadOnlyAccess 181
Utilizzo di questa politica 181
Dettagli della policy 181
Versione della politica 181
Documento di policy JSON 181
Ulteriori informazioni 182
AmazonAppStreamServiceAccess 182
Utilizzo di questa politica 182
Dettagli della policy 182
Versione della politica 182
Documento di policy JSON 183
Ulteriori informazioni 184
AmazonAthenaFullAccess 184
Utilizzo di questa politica 184
Dettagli della policy 184
Versione della politica 184
Documento di policy JSON 185
Ulteriori informazioni 188
AmazonAthenaServiceRolePolicy 188
Utilizzo di questa politica 188
Dettagli della policy 188
Versione della politica 189
Documento di policy JSON 189
Ulteriori informazioni 189

AmazonAugmentedAIFullAccess 190
Utilizzo di questa politica 190
Dettagli della policy 190
Versione della politica 190
Documento di policy JSON 190
Ulteriori informazioni 191
AmazonAugmentedAIHumanLoopFullAccess 192
Utilizzo di questa politica 192
Dettagli della policy 192
Versione della politica 192
Documento di policy JSON 192
Ulteriori informazioni 193
AmazonAugmentedAIIntegratedAPIAccess 193
Utilizzo di questa politica 193
Dettagli della policy 193
Versione della politica 193
Documento di policy JSON 194
Ulteriori informazioni 195
AmazonAuroraDSQLConsoleFullAccess 195
Utilizzo di questa politica 195
Dettagli della policy 195
Versione della politica 196
Documento di policy JSON 196
Ulteriori informazioni 198
AmazonAuroraDSQLFullAccess 198
Utilizzo di questa politica 199
Dettagli della policy 199
Versione della politica 199
Documento di policy JSON 199
Ulteriori informazioni 202
AmazonAuroraDSQLReadOnlyAccess 202
Utilizzo di questa politica 202
Dettagli della policy 202
Versione della politica 202
Documento di policy JSON 203
Ulteriori informazioni 203

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy 204
Utilizzo di questa politica 204
Dettagli della policy 204
Versione della politica 204
Documento sulla politica JSON 204
Ulteriori informazioni 205
AmazonBedrockExternalWebSearchFullAccess 206
Utilizzo di questa politica 206
Dettagli della policy 206
Versione della politica 206
Documento sulla politica JSON 206
Ulteriori informazioni 207
AmazonBedrockExternalWebSearchReadOnly 207
Utilizzo di questa politica 207
Dettagli della policy 207
Versione della politica 207
Documento sulla politica JSON 208
Ulteriori informazioni 208
AmazonBedrockFullAccess 208
Utilizzo di questa politica 208
Dettagli della policy 209
Versione della politica 209
Documento sulla politica JSON 209
Ulteriori informazioni 214
AmazonBedrockLimitedAccess 215
Utilizzo di questa politica 215
Dettagli della policy 215
Versione della politica 215
Documento sulla politica JSON 215
Ulteriori informazioni 218
AmazonBedrockMantleFullAccess 218
Utilizzo di questa politica 218
Dettagli della policy 218
Versione della politica 219
Documento sulla politica JSON 219
Ulteriori informazioni 220

AmazonBedrockMantleInferenceAccess 220
Utilizzo di questa politica 220
Dettagli della policy 220
Versione della politica 220
Documento sulla politica JSON 221
Ulteriori informazioni 222
AmazonBedrockMantleReadOnly 222
Utilizzo di questa politica 222
Dettagli della policy 222
Versione della politica 222
Documento di policy JSON 223
Ulteriori informazioni 223
AmazonBedrockMarketplaceAccess 223
Utilizzo di questa politica 224
Dettagli della policy 224
Versione della politica 224
Documento di policy JSON 224
Ulteriori informazioni 228
AmazonBedrockReadOnly 229
Utilizzo di questa politica 229
Dettagli della policy 229
Versione della politica 229
Documento di policy JSON 229
Ulteriori informazioni 231
AmazonBedrockStudioPermissionsBoundary 231
Utilizzo di questa politica 231
Dettagli della policy 231
Versione della politica 231
Documento di policy JSON 231
Ulteriori informazioni 236
AmazonBedrockWebSearchFullAccess 236
Utilizzo di questa politica 236
Dettagli della policy 236
Versione della politica 236
Documento sulla politica JSON 236
Ulteriori informazioni 237

AmazonBedrockWebSearchReadOnly 237
Utilizzo di questa politica 237
Dettagli della policy 237
Versione della politica 238
Documento sulla politica JSON 238
Ulteriori informazioni 238
AmazonBraketFullAccess 238
Utilizzo di questa politica 239
Dettagli della policy 239
Versione della politica 239
Documento di policy JSON 239
Ulteriori informazioni 244
AmazonBraketJobsExecutionPolicy 244
Utilizzo di questa politica 244
Dettagli della policy 244
Versione della politica 244
Documento di policy JSON 245
Ulteriori informazioni 247
AmazonBraketServiceRolePolicy 248
Utilizzo di questa politica 248
Dettagli della policy 248
Versione della politica 248
Documento di policy JSON 248
Ulteriori informazioni 250
AmazonChimeFullAccess 250
Utilizzo di questa politica 250
Dettagli della policy 250
Versione della politica 250
Documento di policy JSON 250
Ulteriori informazioni 253
AmazonChimeReadOnly 253
Utilizzo di questa politica 253
Dettagli della policy 253
Versione della politica 253
Documento di policy JSON 253
Ulteriori informazioni 254

AmazonChimeSDK 254
Utilizzo di questa politica 254
Dettagli della policy 254
Versione della politica 255
Documento di policy JSON 255
Ulteriori informazioni 256
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 256
Utilizzo di questa politica 256
Dettagli della policy 256
Versione della politica 256
Documento di policy JSON 257
Ulteriori informazioni 258
AmazonChimeSDKMessagingServiceRolePolicy 258
Utilizzo di questa politica 258
Dettagli della policy 258
Versione della politica 259
Documento di policy JSON 259
Ulteriori informazioni 260
AmazonChimeServiceRolePolicy 260
Utilizzo di questa politica 260
Dettagli della policy 260
Versione della politica 260
Documento di policy JSON 260
Ulteriori informazioni 261
AmazonChimeTranscriptionServiceLinkedRolePolicy 261
Utilizzo di questa politica 261
Dettagli della policy 261
Versione della politica 262
Documento di policy JSON 262
Ulteriori informazioni 262
AmazonChimeUserManagement 262
Utilizzo di questa politica 263
Dettagli della policy 263
Versione della politica 263
Documento di policy JSON 263
Ulteriori informazioni 264

AmazonChimeVoiceConnectorServiceLinkedRolePolicy 264
Utilizzo di questa politica 265
Dettagli della policy 265
Versione della politica 265
Documento di policy JSON 265
Ulteriori informazioni 267
AmazonCloudDirectoryFullAccess 267
Utilizzo di questa politica 267
Dettagli della policy 267
Versione della politica 268
Documento di policy JSON 268
Ulteriori informazioni 268
AmazonCloudDirectoryReadOnlyAccess 268
Utilizzo di questa politica 269
Dettagli della policy 269
Versione della politica 269
Documento di policy JSON 269
Ulteriori informazioni 270
AmazonCloudWatchEvidentlyFullAccess 270
Utilizzo di questa politica 270
Dettagli della policy 270
Versione della politica 270
Documento di policy JSON 270
Ulteriori informazioni 273
AmazonCloudWatchEvidentlyReadOnlyAccess 273
Utilizzo di questa politica 273
Dettagli della policy 273
Versione della politica 274
Documento di policy JSON 274
Ulteriori informazioni 274
AmazonCloudWatchEvidentlyServiceRolePolicy 275
Utilizzo di questa politica 275
Dettagli della policy 275
Versione della politica 275
Documento di policy JSON 275
Ulteriori informazioni 277

AmazonCloudWatchRUMFullAccess 277
Utilizzo di questa politica 277
Dettagli della policy 277
Versione della politica 277
Documento di policy JSON 277
Ulteriori informazioni 280
AmazonCloudWatchRUMReadOnlyAccess 280
Utilizzo di questa politica 280
Dettagli della policy 280
Versione della politica 281
Documento di policy JSON 281
Ulteriori informazioni 282
AmazonCloudWatchRUMServiceRolePolicy 282
Utilizzo di questa politica 282
Dettagli della policy 283
Versione della politica 283
Documento di policy JSON 283
Ulteriori informazioni 284
AmazonCodeCatalystFullAccess 284
Utilizzo di questa politica 284
Dettagli della policy 284
Versione della politica 284
Documento di policy JSON 285
Ulteriori informazioni 285
AmazonCodeCatalystReadOnlyAccess 286
Utilizzo di questa politica 286
Dettagli della policy 286
Versione della politica 286
Documento di policy JSON 286
Ulteriori informazioni 287
AmazonCodeCatalystSupportAccess 287
Utilizzo di questa politica 287
Dettagli della policy 287
Versione della politica 287
Documento di policy JSON 287
Ulteriori informazioni 288

AmazonCodeGuruProfilerAgentAccess 288
Utilizzo di questa politica 289
Dettagli della policy 289
Versione della politica 289
Documento di policy JSON 289
Ulteriori informazioni 289
AmazonCodeGuruProfilerFullAccess 290
Utilizzo di questa politica 290
Dettagli della policy 290
Versione della politica 290
Documento di policy JSON 290
Ulteriori informazioni 291
AmazonCodeGuruProfilerReadOnlyAccess 291
Utilizzo di questa politica 291
Dettagli della policy 292
Versione della politica 292
Documento di policy JSON 292
Ulteriori informazioni 292
AmazonCodeGuruReviewerFullAccess 293
Utilizzo di questa politica 293
Dettagli della policy 293
Versione della politica 293
Documento di policy JSON 293
Ulteriori informazioni 296
AmazonCodeGuruReviewerReadOnlyAccess 296
Utilizzo di questa politica 296
Dettagli della policy 296
Versione della politica 297
Documento di policy JSON 297
Ulteriori informazioni 297
AmazonCodeGuruReviewerServiceRolePolicy 297
Utilizzo di questa politica 298
Dettagli della policy 298
Versione della politica 298
Documento di policy JSON 298
Ulteriori informazioni 300

AmazonCodeGuruSecurityFullAccess 300
Utilizzo di questa politica 300
Dettagli della policy 300
Versione della politica 301
Documento di policy JSON 301
Ulteriori informazioni 301
AmazonCodeGuruSecurityScanAccess 302
Utilizzo di questa politica 302
Dettagli della policy 302
Versione della politica 302
Documento di policy JSON 302
Ulteriori informazioni 303
AmazonCognitoDeveloperAuthenticatedIdentities 303
Utilizzo di questa politica 303
Dettagli della policy 303
Versione della politica 303
Documento di policy JSON 304
Ulteriori informazioni 304
AmazonCognitoIdpEmailServiceRolePolicy 304
Utilizzo di questa politica 305
Dettagli della policy 305
Versione della politica 305
Documento di policy JSON 305
Ulteriori informazioni 306
AmazonCognitoIdpServiceRolePolicy 306
Utilizzo di questa politica 306
Dettagli della policy 306
Versione della politica 306
Documento di policy JSON 307
Ulteriori informazioni 307
AmazonCognitoPowerUser 307
Utilizzo di questa politica 307
Dettagli della policy 307
Versione della politica 308
Documento di policy JSON 308
Ulteriori informazioni 309

AmazonCognitoReadOnly 309
Utilizzo di questa politica 309
Dettagli della policy 310
Versione della politica 310
Documento di policy JSON 310
Ulteriori informazioni 311
AmazonCognitoUnAuthedIdentitiesSessionPolicy 311
Utilizzo di questa politica 311
Dettagli della policy 311
Versione della politica 312
Documento di policy JSON 312
Ulteriori informazioni 313
AmazonCognitoUnauthenticatedIdentities 313
Utilizzo di questa politica 313
Dettagli della policy 313
Versione della politica 314
Documento di policy JSON 314
Ulteriori informazioni 314
AmazonConnect_FullAccess 314
Utilizzo di questa politica 314
Dettagli della policy 315
Versione della politica 315
Documento di policy JSON 315
Ulteriori informazioni 318
AmazonConnectCampaignsServiceLinkedRolePolicy 318
Utilizzo di questa politica 318
Dettagli della policy 318
Versione della politica 318
Documento di policy JSON 318
Ulteriori informazioni 322
AmazonConnectReadOnlyAccess 322
Utilizzo di questa politica 322
Dettagli della policy 322
Versione della politica 323
Documento di policy JSON 323
Ulteriori informazioni 323

AmazonConnectServiceLinkedRolePolicy 324
Utilizzo di questa politica 324
Dettagli della policy 324
Versione della politica 324
Documento di policy JSON 324
Ulteriori informazioni 333
AmazonConnectSynchronizationServiceRolePolicy 333
Utilizzo di questa politica 333
Dettagli della policy 333
Versione della politica 334
Documento di policy JSON 334
Ulteriori informazioni 336
AmazonConnectVoiceIDFullAccess 336
Utilizzo di questa politica 336
Dettagli della policy 336
Versione della politica 336
Documento di policy JSON 336
Ulteriori informazioni 337
AmazonDataZoneBedrockModelConsumptionPolicy 337
Utilizzo di questa politica 337
Dettagli della policy 337
Versione della politica 338
Documento di policy JSON 338
Ulteriori informazioni 340
AmazonDataZoneBedrockModelManagementPolicy 340
Utilizzo di questa politica 341
Dettagli della policy 341
Versione della politica 341
Documento di policy JSON 341
Ulteriori informazioni 343
AmazonDataZoneDomainExecutionRolePolicy 343
Utilizzo di questa politica 343
Dettagli della policy 343
Versione della politica 344
Documento di policy JSON 344
Ulteriori informazioni 347

AmazonDataZoneEnvironmentRolePermissionsBoundary 348
Utilizzo di questa politica 348
Dettagli della policy 348
Versione della politica 348
Documento di policy JSON 348
Ulteriori informazioni 361
AmazonDataZoneFullAccess 361
Utilizzo di questa politica 361
Dettagli della policy 362
Versione della politica 362
Documento di policy JSON 362
Ulteriori informazioni 371
AmazonDataZoneFullUserAccess 371
Utilizzo di questa politica 371
Dettagli della policy 371
Versione della politica 372
Documento di policy JSON 372
Ulteriori informazioni 375
AmazonDataZoneGlueManageAccessRolePolicy 375
Utilizzo di questa politica 376
Dettagli della policy 376
Versione della politica 376
Documento di policy JSON 376
Ulteriori informazioni 384
AmazonDataZonePortalFullAccessPolicy 384
Utilizzo di questa politica 384
Dettagli della policy 384
Versione della politica 385
Documento di policy JSON 385
Ulteriori informazioni 385
AmazonDataZonePreviewConsoleFullAccess 385
Utilizzo di questa politica 385
Dettagli della policy 386
Versione della politica 386
Documento di policy JSON 386
Ulteriori informazioni 388

AmazonDataZoneProjectDeploymentPermissionsBoundary 388
Utilizzo di questa politica 388
Dettagli della policy 388
Versione della politica 389
Documento di policy JSON 389
Ulteriori informazioni 397
AmazonDataZoneProjectRolePermissionsBoundary 397
Utilizzo di questa politica 397
Dettagli della policy 397
Versione della politica 397
Documento di policy JSON 398
Ulteriori informazioni 405
AmazonDataZoneRedshiftGlueProvisioningPolicy 405
Utilizzo di questa politica 405
Dettagli della policy 405
Versione della politica 406
Documento di policy JSON 406
Ulteriori informazioni 413
AmazonDataZoneRedshiftManageAccessRolePolicy 414
Utilizzo di questa politica 414
Dettagli della policy 414
Versione della politica 414
Documento di policy JSON 414
Ulteriori informazioni 417
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 418
Utilizzo di questa politica 418
Dettagli della policy 418
Versione della politica 418
Documento sulla politica JSON 418
Ulteriori informazioni 446
AmazonDataZoneSageMakerManageAccessRolePolicy 446
Utilizzo di questa politica 446
Dettagli della policy 446
Versione della politica 447
Documento di policy JSON 447
Ulteriori informazioni 451

AmazonDataZoneSageMakerProvisioningRolePolicy 452
Utilizzo di questa politica 452
Dettagli della policy 452
Versione della politica 452
Documento di policy JSON 452
Ulteriori informazioni 457
AmazonDetectiveFullAccess 457
Utilizzo di questa politica 457
Dettagli della policy 457
Versione della politica 458
Documento di policy JSON 458
Ulteriori informazioni 459
AmazonDetectiveInvestigatorAccess 459
Utilizzo di questa politica 459
Dettagli della policy 459
Versione della politica 459
Documento di policy JSON 460
Ulteriori informazioni 461
AmazonDetectiveMemberAccess 461
Utilizzo di questa politica 462
Dettagli della policy 462
Versione della politica 462
Documento di policy JSON 462
Ulteriori informazioni 463
AmazonDetectiveOrganizationsAccess 463
Utilizzo di questa politica 463
Dettagli della policy 463
Versione della politica 463
Documento di policy JSON 464
Ulteriori informazioni 465
AmazonDetectiveServiceLinkedRolePolicy 465
Utilizzo di questa politica 466
Dettagli della policy 466
Versione della politica 466
Documento di policy JSON 466
Ulteriori informazioni 467

AmazonDevOpsGuruConsoleFullAccess 467
Utilizzo di questa politica 467
Dettagli della policy 467
Versione della politica 467
Documento di policy JSON 467
Ulteriori informazioni 470
AmazonDevOpsGuruFullAccess 470
Utilizzo di questa politica 470
Dettagli della policy 470
Versione della politica 470
Documento di policy JSON 471
Ulteriori informazioni 473
AmazonDevOpsGuruOrganizationsAccess 473
Utilizzo di questa politica 473
Dettagli della policy 473
Versione della politica 474
Documento di policy JSON 474
Ulteriori informazioni 475
AmazonDevOpsGuruReadOnlyAccess 475
Utilizzo di questa politica 475
Dettagli della policy 475
Versione della politica 476
Documento di policy JSON 476
Ulteriori informazioni 478
AmazonDevOpsGuruServiceRolePolicy 478
Utilizzo di questa politica 478
Dettagli della policy 478
Versione della politica 478
Documento di policy JSON 479
Ulteriori informazioni 483
AmazonDMSCloudWatchLogsRole 483
Utilizzo di questa politica 483
Dettagli della policy 483
Versione della politica 483
Documento di policy JSON 483
Ulteriori informazioni 485

AmazonDMSRedshiftS3Role 485
Utilizzo di questa politica 485
Dettagli della policy 485
Versione della politica 486
Documento di policy JSON 486
Ulteriori informazioni 486
AmazonDMSVPCManagementRole 487
Utilizzo di questa politica 487
Dettagli della policy 487
Versione della politica 487
Documento di policy JSON 487
Ulteriori informazioni 488
AmazonDocDB-ElasticServiceRolePolicy 488
Utilizzo di questa politica 488
Dettagli della policy 488
Versione della politica 489
Documento di policy JSON 489
Ulteriori informazioni 489
AmazonDocDBConsoleFullAccess 490
Utilizzo di questa politica 490
Dettagli della policy 490
Versione della politica 490
Documento di policy JSON 490
Ulteriori informazioni 495
AmazonDocDBElasticFullAccess 495
Utilizzo di questa politica 495
Dettagli della policy 495
Versione della politica 495
Documento di policy JSON 496
Ulteriori informazioni 499
AmazonDocDBElasticReadOnlyAccess 499
Utilizzo di questa politica 499
Dettagli della policy 499
Versione della politica 499
Documento di policy JSON 500
Ulteriori informazioni 500

AmazonDocDBFullAccess 501
Utilizzo di questa politica 501
Dettagli della policy 501
Versione della politica 501
Documento di policy JSON 501
Ulteriori informazioni 504
AmazonDocDBReadOnlyAccess 504
Utilizzo di questa politica 504
Dettagli della policy 504
Versione della politica 505
Documento di policy JSON 505
Ulteriori informazioni 507
AmazonDRSVPCManagement 507
Utilizzo di questa politica 507
Dettagli della policy 507
Versione della politica 507
Documento di policy JSON 507
Ulteriori informazioni 508
AmazonDynamoDBFullAccess 508
Utilizzo di questa politica 508
Dettagli della policy 509
Versione della politica 509
Documento di policy JSON 509
Ulteriori informazioni 512
AmazonDynamoDBFullAccess_v2 512
Utilizzo di questa politica 512
Dettagli della policy 512
Versione della politica 512
Documento di policy JSON 512
Ulteriori informazioni 516
AmazonDynamoDBFullAccesswithDataPipeline 516
Utilizzo di questa politica 516
Dettagli della policy 516
Versione della politica 516
Documento di policy JSON 517
Ulteriori informazioni 519

AmazonDynamoDBReadOnlyAccess 519
Utilizzo di questa politica 519
Dettagli della policy 519
Versione della politica 519
Documento di policy JSON 520
Ulteriori informazioni 521
AmazonEBSCSIDriverEKSClusterScopedPolicy 521
Utilizzo di questa politica 522
Dettagli della policy 522
Versione della politica 522
Documento di policy JSON 522
Ulteriori informazioni 527
AmazonEBSCSIDriverPolicy 527
Utilizzo di questa politica 528
Dettagli della policy 528
Versione della politica 528
Documento di policy JSON 528
Ulteriori informazioni 533
AmazonEBSCSIDriverPolicyV2 533
Utilizzo di questa politica 533
Dettagli della policy 533
Versione della politica 533
Documento di policy JSON 534
Ulteriori informazioni 538
AmazonEC2ContainerRegistryFullAccess 538
Utilizzo di questa politica 539
Dettagli della policy 539
Versione della politica 539
Documento di policy JSON 539
Ulteriori informazioni 540
AmazonEC2ContainerRegistryPowerUser 540
Utilizzo di questa politica 540
Dettagli della policy 540
Versione della politica 540
Documento di policy JSON 541
Ulteriori informazioni 541

AmazonEC2ContainerRegistryPullOnly 542
Utilizzo di questa politica 542
Dettagli della policy 542
Versione della politica 542
Documento di policy JSON 542
Ulteriori informazioni 543
AmazonEC2ContainerRegistryReadOnly 543
Utilizzo di questa politica 543
Dettagli della policy 543
Versione della politica 543
Documento di policy JSON 544
Ulteriori informazioni 544
AmazonEC2ContainerServiceAutoscaleRole 544
Utilizzo di questa politica 545
Dettagli della policy 545
Versione della politica 545
Documento di policy JSON 545
Ulteriori informazioni 546
AmazonEC2ContainerServiceEventsRole 546
Utilizzo di questa politica 546
Dettagli della policy 546
Versione della politica 546
Documento di policy JSON 547
Ulteriori informazioni 548
AmazonEC2ContainerServiceforEC2Role 548
Utilizzo di questa politica 548
Dettagli della policy 548
Versione della politica 548
Documento di policy JSON 549
Ulteriori informazioni 550
AmazonEC2ContainerServiceRole 550
Utilizzo di questa politica 550
Dettagli della policy 550
Versione della politica 550
Documento di policy JSON 551
Ulteriori informazioni 551

AmazonEC2FullAccess 551
Utilizzo di questa politica 552
Dettagli della policy 552
Versione della politica 552
Documento di policy JSON 552
Ulteriori informazioni 553
AmazonEC2ImageReferencesAccessPolicy 553
Utilizzo di questa politica 554
Dettagli della policy 554
Versione della politica 554
Documento di policy JSON 554
Ulteriori informazioni 555
AmazonEC2ReadOnlyAccess 555
Utilizzo di questa politica 555
Dettagli della policy 555
Versione della politica 556
Documento di policy JSON 556
Ulteriori informazioni 557
AmazonEC2RoleforAWSCodeDeploy 557
Utilizzo di questa politica 557
Dettagli della policy 557
Versione della politica 557
Documento di policy JSON 557
Ulteriori informazioni 558
AmazonEC2RoleforAWSCodeDeployLimited 558
Utilizzo di questa politica 558
Dettagli della policy 558
Versione della politica 559
Documento di policy JSON 559
Ulteriori informazioni 560
AmazonEC2RoleforDataPipelineRole 560
Utilizzo di questa politica 560
Dettagli della policy 560
Versione della politica 560
Documento di policy JSON 560
Ulteriori informazioni 561

AmazonEC2RoleforSSM 561
Utilizzo di questa politica 562
Dettagli della policy 562
Versione della politica 562
Documento di policy JSON 562
Ulteriori informazioni 564
AmazonEC2RolePolicyForLaunchWizard 565
Utilizzo di questa politica 565
Dettagli della policy 565
Versione della politica 565
Documento di policy JSON 565
Ulteriori informazioni 569
AmazonEC2SpotFleetAutoscaleRole 569
Utilizzo di questa politica 569
Dettagli della policy 570
Versione della politica 570
Documento di policy JSON 570
Ulteriori informazioni 571
AmazonEC2SpotFleetTaggingRole 571
Utilizzo di questa politica 571
Dettagli della policy 571
Versione della politica 572
Documento di policy JSON 572
Ulteriori informazioni 573
AmazonECS_FullAccess 573
Utilizzo di questa politica 573
Dettagli della policy 574
Versione della politica 574
Documento di policy JSON 574
Ulteriori informazioni 580
AmazonECSComputeServiceRolePolicy 580
Utilizzo di questa politica 580
Dettagli della policy 580
Versione della politica 580
Documento di policy JSON 581
Ulteriori informazioni 582

AmazonECSInfrastructureRoleforExpressGatewayServices 582
Utilizzo di questa politica 582
Dettagli della policy 583
Versione della politica 583
Documento di policy JSON 583
Ulteriori informazioni 589
AmazonECSInfrastructureRolePolicyForLoadBalancers 590
Utilizzo di questa politica 590
Dettagli della policy 590
Versione della politica 590
Documento di policy JSON 590
Ulteriori informazioni 592
AmazonECSInfrastructureRolePolicyForManagedInstances 592
Utilizzo di questa politica 592
Dettagli della policy 592
Versione della politica 592
Documento di policy JSON 592
Ulteriori informazioni 597
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 597
Utilizzo di questa politica 597
Dettagli della policy 597
Versione della politica 598
Documento di policy JSON 598
Ulteriori informazioni 600
AmazonECSInfrastructureRolePolicyForVolumes 601
Utilizzo di questa politica 601
Dettagli della policy 601
Versione della politica 601
Documento di policy JSON 601
Ulteriori informazioni 604
AmazonECSInfrastructureRolePolicyForVpcLattice 604
Utilizzo di questa politica 604
Dettagli della policy 604
Versione della politica 604
Documento di policy JSON 605
Ulteriori informazioni 606

AmazonECSInstanceRolePolicyForManagedInstances 606
Utilizzo di questa politica 606
Dettagli della policy 606
Versione della politica 606
Documento di policy JSON 607
Ulteriori informazioni 608
AmazonECSServiceRolePolicy 608
Utilizzo di questa politica 608
Dettagli della policy 608
Versione della politica 609
Documento di policy JSON 609
Ulteriori informazioni 614
AmazonECSTaskExecutionRolePolicy 615
Utilizzo di questa politica 615
Dettagli della policy 615
Versione della politica 615
Documento di policy JSON 615
Ulteriori informazioni 616
AmazonEFSCSIDriverPolicy 616
Utilizzo di questa politica 616
Dettagli della policy 616
Versione della politica 616
Documento di policy JSON 617
Ulteriori informazioni 618
AmazonEKS_CNI_Policy 618
Utilizzo di questa politica 619
Dettagli della policy 619
Versione della politica 619
Documento di policy JSON 619
Ulteriori informazioni 620
AmazonEKSBlockStoragePolicy 620
Utilizzo di questa politica 620
Dettagli della policy 620
Versione della politica 621
Documento di policy JSON 621
Ulteriori informazioni 623

AmazonEKSBlockStoragePolicyV2 623
Utilizzo di questa politica 624
Dettagli della policy 624
Versione della politica 624
Documento di policy JSON 624
Ulteriori informazioni 627
AmazonEKSClusterPolicy 627
Utilizzo di questa politica 627
Dettagli della policy 627
Versione della politica 627
Documento di policy JSON 628
Ulteriori informazioni 630
AmazonEKSComputePolicy 630
Utilizzo di questa politica 630
Dettagli della policy 630
Versione della politica 631
Documento di policy JSON 631
Ulteriori informazioni 633
AmazonEKSConnectorServiceRolePolicy 634
Utilizzo di questa politica 634
Dettagli della policy 634
Versione della politica 634
Documento di policy JSON 634
Ulteriori informazioni 636
AmazonEKSDashboardConsoleReadOnly 636
Utilizzo di questa politica 637
Dettagli della policy 637
Versione della politica 637
Documento di policy JSON 637
Ulteriori informazioni 638
AmazonEKSDashboardServiceRolePolicy 638
Utilizzo di questa politica 639
Dettagli della policy 639
Versione della politica 639
Documento di policy JSON 639
Ulteriori informazioni 640

AmazonEKSFargatePodExecutionRolePolicy 640
Utilizzo di questa politica 640
Dettagli della policy 640
Versione della politica 640
Documento di policy JSON 640
Ulteriori informazioni 641
AmazonEKSForFargateServiceRolePolicy 641
Utilizzo di questa politica 641
Dettagli della policy 641
Versione della politica 642
Documento di policy JSON 642
Ulteriori informazioni 642
AmazonEKSLoadBalancingPolicy 643
Utilizzo di questa politica 643
Dettagli della policy 643
Versione della politica 643
Documento di policy JSON 643
Ulteriori informazioni 649
AmazonEKSLocalOutpostClusterPolicy 649
Utilizzo di questa politica 649
Dettagli della policy 649
Versione della politica 649
Documento di policy JSON 650
Ulteriori informazioni 651
AmazonEKSLocalOutpostServiceRolePolicy 652
Utilizzo di questa politica 652
Dettagli della policy 652
Versione della politica 652
Documento di policy JSON 652
Ulteriori informazioni 658
AmazonEKSMCPReadOnlyAccess 658
Utilizzo di questa politica 658
Dettagli della policy 658
Versione della politica 659
Documento di policy JSON 659
Ulteriori informazioni 661

AmazonEKSNetworkingPolicy 661
Utilizzo di questa politica 661
Dettagli della policy 661
Versione della politica 661
Documento di policy JSON 661
Ulteriori informazioni 663
AmazonEKSServicePolicy 664
Utilizzo di questa politica 664
Dettagli della policy 664
Versione della politica 664
Documento di policy JSON 664
Ulteriori informazioni 666
AmazonEKSServiceRolePolicy 666
Utilizzo di questa politica 667
Dettagli della policy 667
Versione della politica 667
Documento di policy JSON 667
Ulteriori informazioni 675
AmazonEKSVPCResourceController 675
Utilizzo di questa politica 675
Dettagli della policy 675
Versione della politica 676
Documento di policy JSON 676
Ulteriori informazioni 676
AmazonEKSWorkerNodeMinimalPolicy 677
Utilizzo di questa politica 677
Dettagli della policy 677
Versione della politica 677
Documento di policy JSON 677
Ulteriori informazioni 678
AmazonEKSWorkerNodePolicy 678
Utilizzo di questa politica 678
Dettagli della policy 678
Versione della politica 678
Documento di policy JSON 679
Ulteriori informazioni 679

AmazonElastiCacheFullAccess 679
Utilizzo di questa politica 680
Dettagli della policy 680
Versione della politica 680
Documento di policy JSON 680
Ulteriori informazioni 683
AmazonElastiCacheReadOnlyAccess 684
Utilizzo di questa politica 684
Dettagli della policy 684
Versione della politica 684
Documento di policy JSON 684
Ulteriori informazioni 685
AmazonElasticContainerRegistryPublicFullAccess 685
Utilizzo di questa politica 685
Dettagli della policy 685
Versione della politica 685
Documento di policy JSON 686
Ulteriori informazioni 686
AmazonElasticContainerRegistryPublicPowerUser 686
Utilizzo di questa politica 686
Dettagli della policy 686
Versione della politica 687
Documento di policy JSON 687
Ulteriori informazioni 688
AmazonElasticContainerRegistryPublicReadOnly 688
Utilizzo di questa politica 688
Dettagli della policy 688
Versione della politica 688
Documento di policy JSON 688
Ulteriori informazioni 689
AmazonElasticFileSystemClientFullAccess 689
Utilizzo di questa politica 689
Dettagli della policy 690
Versione della politica 690
Documento di policy JSON 690
Ulteriori informazioni 690

AmazonElasticFileSystemClientReadOnlyAccess 691
Utilizzo di questa politica 691
Dettagli della policy 691
Versione della politica 691
Documento di policy JSON 691
Ulteriori informazioni 692
AmazonElasticFileSystemClientReadWriteAccess 692
Utilizzo di questa politica 692
Dettagli della policy 692
Versione della politica 692
Documento di policy JSON 693
Ulteriori informazioni 693
AmazonElasticFileSystemFullAccess 693
Utilizzo di questa politica 693
Dettagli della policy 693
Versione della politica 694
Documento di policy JSON 694
Ulteriori informazioni 696
AmazonElasticFileSystemReadOnlyAccess 696
Utilizzo di questa politica 696
Dettagli della policy 696
Versione della politica 697
Documento di policy JSON 697
Ulteriori informazioni 698
AmazonElasticFileSystemServiceRolePolicy 698
Utilizzo di questa politica 698
Dettagli della policy 698
Versione della politica 698
Documento di policy JSON 699
Ulteriori informazioni 701
AmazonElasticFileSystemsUtils 701
Utilizzo di questa politica 701
Dettagli della policy 701
Versione della politica 701
Documento di policy JSON 701
Ulteriori informazioni 704

AmazonElasticMapReduceEditorsRole 704
Utilizzo di questa politica 704
Dettagli della policy 704
Versione della politica 704
Documento di policy JSON 704
Ulteriori informazioni 706
AmazonElasticMapReduceforAutoScalingRole 706
Utilizzo di questa politica 706
Dettagli della policy 706
Versione della politica 706
Documento di policy JSON 707
Ulteriori informazioni 707
AmazonElasticMapReduceforEC2Role 707
Utilizzo di questa politica 707
Dettagli della policy 707
Versione della politica 708
Documento di policy JSON 708
Ulteriori informazioni 709
AmazonElasticMapReduceFullAccess 709
Utilizzo di questa politica 710
Dettagli della policy 710
Versione della politica 710
Documento di policy JSON 710
Ulteriori informazioni 712
AmazonElasticMapReducePlacementGroupPolicy 712
Utilizzo di questa politica 712
Dettagli della policy 712
Versione della politica 712
Documento di policy JSON 713
Ulteriori informazioni 713
AmazonElasticMapReduceReadOnlyAccess 713
Utilizzo di questa politica 714
Dettagli della policy 714
Versione della politica 714
Documento di policy JSON 714
Ulteriori informazioni 715

AmazonElasticMapReduceRole 715
Utilizzo di questa politica 715
Dettagli della policy 715
Versione della politica 715
Documento di policy JSON 716
Ulteriori informazioni 718
AmazonElasticsearchServiceRolePolicy 718
Utilizzo di questa politica 718
Dettagli della policy 718
Versione della politica 718
Documento di policy JSON 719
Ulteriori informazioni 722
AmazonElasticTranscoder_FullAccess 722
Utilizzo di questa politica 722
Dettagli della policy 722
Versione della politica 722
Documento di policy JSON 722
Ulteriori informazioni 723
AmazonElasticTranscoder_JobsSubmitter 723
Utilizzo di questa politica 724
Dettagli della policy 724
Versione della politica 724
Documento di policy JSON 724
Ulteriori informazioni 725
AmazonElasticTranscoder_ReadOnlyAccess 725
Utilizzo di questa politica 725
Dettagli della policy 725
Versione della politica 725
Documento di policy JSON 726
Ulteriori informazioni 726
AmazonElasticTranscoderRole 726
Utilizzo di questa politica 726
Dettagli della policy 727
Versione della politica 727
Documento di policy JSON 727
Ulteriori informazioni 728

AmazonEMRCleanupPolicy 728
Utilizzo di questa politica 728
Dettagli della policy 728
Versione della politica 728
Documento di policy JSON 729
Ulteriori informazioni 729
AmazonEMRContainersServiceRolePolicy 730
Utilizzo di questa politica 730
Dettagli della policy 730
Versione della politica 730
Documento sulla politica JSON 730
Ulteriori informazioni 733
AmazonEMRFullAccessPolicy_v2 733
Utilizzo di questa politica 733
Dettagli della policy 733
Versione della politica 733
Documento di policy JSON 734
Ulteriori informazioni 737
AmazonEMRReadOnlyAccessPolicy_v2 737
Utilizzo di questa politica 737
Dettagli della policy 737
Versione della politica 738
Documento di policy JSON 738
Ulteriori informazioni 739
AmazonEMRServerlessServiceRolePolicy 739
Utilizzo di questa politica 739
Dettagli della policy 739
Versione della politica 740
Documento di policy JSON 740
Ulteriori informazioni 741
AmazonEMRServicePolicy_v2 741
Utilizzo di questa politica 741
Dettagli della policy 741
Versione della politica 741
Documento di policy JSON 742
Ulteriori informazioni 750

AmazonEMRServicePolicyForSessions 751
Utilizzo di questa politica 751
Dettagli della policy 751
Versione della politica 751
Documento di policy JSON 751
Ulteriori informazioni 755
AmazonESCognitoAccess 755
Utilizzo di questa politica 755
Dettagli della policy 755
Versione della politica 756
Documento di policy JSON 756
Ulteriori informazioni 757
AmazonESFullAccess 757
Utilizzo di questa politica 757
Dettagli della policy 757
Versione della politica 757
Documento di policy JSON 758
Ulteriori informazioni 758
AmazonESReadOnlyAccess 758
Utilizzo di questa politica 758
Dettagli della policy 758
Versione della politica 759
Documento di policy JSON 759
Ulteriori informazioni 759
AmazonEventBridgeApiDestinationsServiceRolePolicy 759
Utilizzo di questa politica 760
Dettagli della policy 760
Versione della politica 760
Documento di policy JSON 760
Ulteriori informazioni 761
AmazonEventBridgeFullAccess 761
Utilizzo di questa politica 761
Dettagli della policy 762
Versione della politica 762
Documento di policy JSON 762
Ulteriori informazioni 764

AmazonEventBridgePipesFullAccess 764
Utilizzo di questa politica 764
Dettagli della policy 764
Versione della politica 765
Documento di policy JSON 765
Ulteriori informazioni 765
AmazonEventBridgePipesOperatorAccess 766
Utilizzo di questa politica 766
Dettagli della policy 766
Versione della politica 766
Documento di policy JSON 766
Ulteriori informazioni 767
AmazonEventBridgePipesReadOnlyAccess 767
Utilizzo di questa politica 767
Dettagli della policy 767
Versione della politica 768
Documento di policy JSON 768
Ulteriori informazioni 768
AmazonEventBridgeReadOnlyAccess 768
Utilizzo di questa politica 769
Dettagli della policy 769
Versione della politica 769
Documento di policy JSON 769
Ulteriori informazioni 770
AmazonEventBridgeSchedulerFullAccess 771
Utilizzo di questa politica 771
Dettagli della policy 771
Versione della politica 771
Documento di policy JSON 771
Ulteriori informazioni 772
AmazonEventBridgeSchedulerReadOnlyAccess 772
Utilizzo di questa politica 772
Dettagli della policy 772
Versione della politica 773
Documento di policy JSON 773
Ulteriori informazioni 773

AmazonEventBridgeSchemasFullAccess 773
Utilizzo di questa politica 774
Dettagli della policy 774
Versione della politica 774
Documento di policy JSON 774
Ulteriori informazioni 775
AmazonEventBridgeSchemasReadOnlyAccess 775
Utilizzo di questa politica 775
Dettagli della policy 775
Versione della politica 776
Documento di policy JSON 776
Ulteriori informazioni 776
AmazonEventBridgeSchemasServiceRolePolicy 777
Utilizzo di questa politica 777
Dettagli della policy 777
Versione della politica 777
Documento di policy JSON 777
Ulteriori informazioni 778
AmazonEVSServiceRolePolicy 778
Utilizzo di questa politica 778
Dettagli della policy 778
Versione della politica 779
Documento di policy JSON 779
Ulteriori informazioni 784
AmazonFISServiceRolePolicy 784
Utilizzo di questa politica 784
Dettagli della policy 784
Versione della politica 785
Documento di policy JSON 785
Ulteriori informazioni 786
AmazonForecastFullAccess 787
Utilizzo di questa politica 787
Dettagli della policy 787
Versione della politica 787
Documento di policy JSON 787
Ulteriori informazioni 788

AmazonFraudDetectorFullAccessPolicy 788
Utilizzo di questa politica 788
Dettagli della policy 788
Versione della politica 789
Documento di policy JSON 789
Ulteriori informazioni 790
AmazonFreeRTOSFullAccess 790
Utilizzo di questa politica 790
Dettagli della policy 790
Versione della politica 791
Documento di policy JSON 791
Ulteriori informazioni 791
AmazonFreeRTOSOTAUpdate 791
Utilizzo di questa politica 791
Dettagli della policy 792
Versione della politica 792
Documento di policy JSON 792
Ulteriori informazioni 793
AmazonFSxConsoleFullAccess 794
Utilizzo di questa politica 794
Dettagli della policy 794
Versione della politica 794
Documento di policy JSON 794
Ulteriori informazioni 798
AmazonFSxConsoleReadOnlyAccess 798
Utilizzo di questa politica 798
Dettagli della policy 798
Versione della politica 798
Documento di policy JSON 799
Ulteriori informazioni 799
AmazonFSxFullAccess 799
Utilizzo di questa politica 800
Dettagli della policy 800
Versione della politica 800
Documento di policy JSON 800
Ulteriori informazioni 804

AmazonFSxReadOnlyAccess 804
Utilizzo di questa politica 805
Dettagli della policy 805
Versione della politica 805
Documento di policy JSON 805
Ulteriori informazioni 805
AmazonFSxServiceRolePolicy 806
Utilizzo di questa politica 806
Dettagli della policy 806
Versione della politica 806
Documento di policy JSON 806
Ulteriori informazioni 809
AmazonGlacierFullAccess 809
Utilizzo di questa politica 809
Dettagli della policy 809
Versione della politica 810
Documento di policy JSON 810
Ulteriori informazioni 810
AmazonGlacierReadOnlyAccess 810
Utilizzo di questa politica 811
Dettagli della policy 811
Versione della politica 811
Documento di policy JSON 811
Ulteriori informazioni 812
AmazonGrafanaAthenaAccess 812
Utilizzo di questa politica 812
Dettagli della policy 812
Versione della politica 812
Documento di policy JSON 813
Ulteriori informazioni 814
AmazonGrafanaCloudWatchAccess 815
Utilizzo di questa politica 815
Dettagli della policy 815
Versione della politica 815
Documento di policy JSON 815
Ulteriori informazioni 817

AmazonGrafanaRedshiftAccess 817
Utilizzo di questa politica 817
Dettagli della policy 817
Versione della politica 817
Documento di policy JSON 817
Ulteriori informazioni 819
AmazonGrafanaServiceLinkedRolePolicy 819
Utilizzo di questa politica 819
Dettagli della policy 819
Versione della politica 819
Documento di policy JSON 820
Ulteriori informazioni 821
AmazonGuardDutyFullAccess 821
Utilizzo di questa politica 821
Dettagli della policy 821
Versione della politica 822
Documento di policy JSON 822
Ulteriori informazioni 823
AmazonGuardDutyFullAccess_v2 823
Utilizzo di questa politica 824
Dettagli della policy 824
Versione della politica 824
Documento di policy JSON 824
Ulteriori informazioni 826
AmazonGuardDutyMalwareProtectionServiceRolePolicy 826
Utilizzo di questa politica 827
Dettagli della policy 827
Versione della politica 827
Documento di policy JSON 827
Ulteriori informazioni 831
AmazonGuardDutyReadOnlyAccess 832
Utilizzo di questa politica 832
Dettagli della policy 832
Versione della politica 832
Documento di policy JSON 832
Ulteriori informazioni 833

AmazonGuardDutyServiceRolePolicy 833
Utilizzo di questa politica 833
Dettagli della policy 833
Versione della politica 834
Documento di policy JSON 834
Ulteriori informazioni 840
AmazonHealthLakeFullAccess 840
Utilizzo di questa politica 841
Dettagli della policy 841
Versione della politica 841
Documento di policy JSON 841
Ulteriori informazioni 842
AmazonHealthLakeReadOnlyAccess 842
Utilizzo di questa politica 842
Dettagli della policy 842
Versione della politica 842
Documento di policy JSON 843
Ulteriori informazioni 843
AmazonHoneycodeFullAccess 843
Utilizzo di questa politica 844
Dettagli della policy 844
Versione della politica 844
Documento di policy JSON 844
Ulteriori informazioni 844
AmazonHoneycodeReadOnlyAccess 845
Utilizzo di questa politica 845
Dettagli della policy 845
Versione della politica 845
Documento di policy JSON 845
Ulteriori informazioni 846
AmazonHoneycodeServiceRolePolicy 846
Utilizzo di questa politica 846
Dettagli della policy 846
Versione della politica 846
Documento di policy JSON 847
Ulteriori informazioni 847

AmazonHoneycodeTeamAssociationFullAccess 847
Utilizzo di questa politica 847
Dettagli della policy 847
Versione della politica 848
Documento di policy JSON 848
Ulteriori informazioni 848
AmazonHoneycodeTeamAssociationReadOnlyAccess 849
Utilizzo di questa politica 849
Dettagli della policy 849
Versione della politica 849
Documento di policy JSON 849
Ulteriori informazioni 850
AmazonHoneycodeWorkbookFullAccess 850
Utilizzo di questa politica 850
Dettagli della policy 850
Versione della politica 850
Documento di policy JSON 851
Ulteriori informazioni 851
AmazonHoneycodeWorkbookReadOnlyAccess 851
Utilizzo di questa politica 852
Dettagli della policy 852
Versione della politica 852
Documento di policy JSON 852
Ulteriori informazioni 853
AmazonInspector2AgentlessServiceRolePolicy 853
Utilizzo di questa politica 853
Dettagli della policy 853
Versione della politica 853
Documento di policy JSON 854
Ulteriori informazioni 857
AmazonInspector2AmiScanServiceRolePolicy 857
Utilizzo di questa politica 857
Dettagli della policy 858
Versione della politica 858
Documento sulla politica JSON 858
Ulteriori informazioni 862

AmazonInspector2FullAccess 862
Utilizzo di questa politica 862
Dettagli della policy 862
Versione della politica 862
Documento di policy JSON 862
Ulteriori informazioni 864
AmazonInspector2FullAccess_v2 864
Utilizzo di questa politica 864
Dettagli della policy 864
Versione della politica 864
Documento di policy JSON 864
Ulteriori informazioni 868
AmazonInspector2ManagedCisPolicy 868
Utilizzo di questa politica 868
Dettagli della policy 868
Versione della politica 868
Documento di policy JSON 869
Ulteriori informazioni 869
AmazonInspector2ManagedTelemetryPolicy 869
Utilizzo di questa politica 869
Dettagli della policy 870
Versione della politica 870
Documento di policy JSON 870
Ulteriori informazioni 870
AmazonInspector2ReadOnlyAccess 871
Utilizzo di questa politica 871
Dettagli della policy 871
Versione della politica 871
Documento di policy JSON 871
Ulteriori informazioni 873
AmazonInspector2ServiceRolePolicy 873
Utilizzo di questa politica 873
Dettagli della policy 873
Versione della politica 874
Documento di policy JSON 874
Ulteriori informazioni 882

AmazonInspector2ThirdPartyServiceRolePolicy 882
Utilizzo di questa politica 882
Dettagli della policy 882
Versione della politica 883
Documento di policy JSON 883
Ulteriori informazioni 887
AmazonInspectorFullAccess 888
Utilizzo di questa politica 888
Dettagli della policy 888
Versione della politica 888
Documento di policy JSON 888
Ulteriori informazioni 889
AmazonInspectorReadOnlyAccess 889
Utilizzo di questa politica 890
Dettagli della policy 890
Versione della politica 890
Documento di policy JSON 890
Ulteriori informazioni 891
AmazonInspectorServiceRolePolicy 891
Utilizzo di questa politica 891
Dettagli della policy 891
Versione della politica 891
Documento di policy JSON 892
Ulteriori informazioni 893
AmazonKendraFullAccess 893
Utilizzo di questa politica 893
Dettagli della policy 893
Versione della politica 894
Documento di policy JSON 894
Ulteriori informazioni 896
AmazonKendraReadOnlyAccess 896
Utilizzo di questa politica 896
Dettagli della policy 896
Versione della politica 896
Documento di policy JSON 896
Ulteriori informazioni 897

AmazonKeyspacesFullAccess 897
Utilizzo di questa politica 897
Dettagli della policy 897
Versione della politica 898
Documento di policy JSON 898
Ulteriori informazioni 900
AmazonKeyspacesReadOnlyAccess 900
Utilizzo di questa politica 900
Dettagli della policy 900
Versione della politica 901
Documento di policy JSON 901
Ulteriori informazioni 902
AmazonKeyspacesReadOnlyAccess_v2 902
Utilizzo di questa politica 902
Dettagli della policy 902
Versione della politica 902
Documento di policy JSON 902
Ulteriori informazioni 903
AmazonKinesisAnalyticsFullAccess 904
Utilizzo di questa politica 904
Dettagli della policy 904
Versione della politica 904
Documento di policy JSON 904
Ulteriori informazioni 906
AmazonKinesisAnalyticsReadOnly 906
Utilizzo di questa politica 906
Dettagli della policy 906
Versione della politica 906
Documento di policy JSON 907
Ulteriori informazioni 908
AmazonKinesisFirehoseFullAccess 908
Utilizzo di questa politica 908
Dettagli della policy 908
Versione della politica 908
Documento di policy JSON 909
Ulteriori informazioni 909

AmazonKinesisFirehoseReadOnlyAccess 909
Utilizzo di questa politica 909
Dettagli della policy 909
Versione della politica 910
Documento di policy JSON 910
Ulteriori informazioni 910
AmazonKinesisFullAccess 910
Utilizzo di questa politica 911
Dettagli della policy 911
Versione della politica 911
Documento di policy JSON 911
Ulteriori informazioni 911
AmazonKinesisReadOnlyAccess 912
Utilizzo di questa politica 912
Dettagli della policy 912
Versione della politica 912
Documento di policy JSON 912
Ulteriori informazioni 913
AmazonKinesisVideoStreamsFullAccess 913
Utilizzo di questa politica 913
Dettagli della policy 913
Versione della politica 913
Documento di policy JSON 914
Ulteriori informazioni 914
AmazonKinesisVideoStreamsReadOnlyAccess 914
Utilizzo di questa politica 914
Dettagli della policy 914
Versione della politica 915
Documento di policy JSON 915
Ulteriori informazioni 915
AmazonLaunchWizard_Fullaccess 915
Utilizzo di questa politica 916
Dettagli della policy 916
Versione della politica 916
Documento di policy JSON 916
Ulteriori informazioni 930

AmazonLaunchWizardFullAccessV2 930
Utilizzo di questa politica 931
Dettagli della policy 931
Versione della politica 931
Documento di policy JSON 931
Ulteriori informazioni 948
AmazonLexChannelsAccess 948
Utilizzo di questa politica 948
Dettagli della policy 948
Versione della politica 948
Documento di policy JSON 948
Ulteriori informazioni 949
AmazonLexFullAccess 949
Utilizzo di questa politica 949
Dettagli della policy 949
Versione della politica 949
Documento di policy JSON 950
Ulteriori informazioni 955
AmazonLexReadOnly 955
Utilizzo di questa politica 955
Dettagli della policy 956
Versione della politica 956
Documento di policy JSON 956
Ulteriori informazioni 957
AmazonLexReplicationPolicy 958
Utilizzo di questa politica 958
Dettagli della policy 958
Versione della politica 958
Documento di policy JSON 958
Ulteriori informazioni 961
AmazonLexRunBotsOnly 961
Utilizzo di questa politica 961
Dettagli della policy 961
Versione della politica 961
Documento di policy JSON 961
Ulteriori informazioni 962

AmazonLexV2BotPolicy 962
Utilizzo di questa politica 962
Dettagli della policy 962
Versione della politica 963
Documento di policy JSON 963
Ulteriori informazioni 963
AmazonLookoutEquipmentFullAccess 963
Utilizzo di questa politica 964
Dettagli della policy 964
Versione della politica 964
Documento di policy JSON 964
Ulteriori informazioni 965
AmazonLookoutEquipmentReadOnlyAccess 965
Utilizzo di questa politica 966
Dettagli della policy 966
Versione della politica 966
Documento di policy JSON 966
Ulteriori informazioni 966
AmazonLookoutMetricsFullAccess 967
Utilizzo di questa politica 967
Dettagli della policy 967
Versione della politica 967
Documento di policy JSON 967
Ulteriori informazioni 968
AmazonLookoutMetricsReadOnlyAccess 968
Utilizzo di questa politica 968
Dettagli della policy 968
Versione della politica 969
Documento di policy JSON 969
Ulteriori informazioni 970
AmazonLookoutVisionConsoleFullAccess 970
Utilizzo di questa politica 970
Dettagli della policy 970
Versione della politica 970
Documento di policy JSON 970
Ulteriori informazioni 973

AmazonLookoutVisionConsoleReadOnlyAccess 973
Utilizzo di questa politica 973
Dettagli della policy 973
Versione della politica 973
Documento di policy JSON 974
Ulteriori informazioni 975
AmazonLookoutVisionFullAccess 975
Utilizzo di questa politica 975
Dettagli della policy 975
Versione della politica 975
Documento di policy JSON 976
Ulteriori informazioni 976
AmazonLookoutVisionReadOnlyAccess 976
Utilizzo di questa politica 976
Dettagli della policy 977
Versione della politica 977
Documento di policy JSON 977
Ulteriori informazioni 978
AmazonMachineLearningBatchPredictionsAccess 978
Utilizzo di questa politica 978
Dettagli della policy 978
Versione della politica 978
Documento di policy JSON 978
Ulteriori informazioni 979
AmazonMachineLearningCreateOnlyAccess 979
Utilizzo di questa politica 979
Dettagli della policy 979
Versione della politica 980
Documento di policy JSON 980
Ulteriori informazioni 980
AmazonMachineLearningFullAccess 980
Utilizzo di questa politica 981
Dettagli della policy 981
Versione della politica 981
Documento di policy JSON 981
Ulteriori informazioni 981

AmazonMachineLearningManageRealTimeEndpointOnlyAccess 982
Utilizzo di questa politica 982
Dettagli della policy 982
Versione della politica 982
Documento di policy JSON 982
Ulteriori informazioni 983
AmazonMachineLearningReadOnlyAccess 983
Utilizzo di questa politica 983
Dettagli della policy 983
Versione della politica 983
Documento di policy JSON 984
Ulteriori informazioni 984
AmazonMachineLearningRealTimePredictionOnlyAccess 984
Utilizzo di questa politica 984
Dettagli della policy 985
Versione della politica 985
Documento di policy JSON 985
Ulteriori informazioni 985
AmazonMachineLearningRoleforRedshiftDataSourceV3 986
Utilizzo di questa politica 986
Dettagli della policy 986
Versione della politica 986
Documento di policy JSON 986
Ulteriori informazioni 987
AmazonMacieFullAccess 987
Utilizzo di questa politica 987
Dettagli della policy 988
Versione della politica 988
Documento di policy JSON 988
Ulteriori informazioni 989
AmazonMacieHandshakeRole 989
Utilizzo di questa politica 989
Dettagli della policy 989
Versione della politica 989
Documento di policy JSON 990
Ulteriori informazioni 990

AmazonMacieReadOnlyAccess 990
Utilizzo di questa politica 990
Dettagli della policy 990
Versione della politica 991
Documento di policy JSON 991
Ulteriori informazioni 991
AmazonMacieServiceRole 992
Utilizzo di questa politica 992
Dettagli della policy 992
Versione della politica 992
Documento di policy JSON 992
Ulteriori informazioni 993
AmazonMacieServiceRolePolicy 993
Utilizzo di questa politica 993
Dettagli della policy 993
Versione della politica 993
Documento di policy JSON 994
Ulteriori informazioni 995
AmazonManagedBlockchainConsoleFullAccess 995
Utilizzo di questa politica 995
Dettagli della policy 995
Versione della politica 996
Documento di policy JSON 996
Ulteriori informazioni 996
AmazonManagedBlockchainFullAccess 996
Utilizzo di questa politica 997
Dettagli della policy 997
Versione della politica 997
Documento di policy JSON 997
Ulteriori informazioni 998
AmazonManagedBlockchainReadOnlyAccess 998
Utilizzo di questa politica 998
Dettagli della policy 998
Versione della politica 998
Documento di policy JSON 998
Ulteriori informazioni 999

AmazonManagedBlockchainServiceRolePolicy 999
Utilizzo di questa politica 999
Dettagli della policy 999
Versione della politica 1000
Documento di policy JSON 1000
Ulteriori informazioni 1000
AmazonMCSFullAccess 1001
Utilizzo di questa politica 1001
Dettagli della policy 1001
Versione della politica 1001
Documento di policy JSON 1001
Ulteriori informazioni 1002
AmazonMCSReadOnlyAccess 1003
Utilizzo di questa politica 1003
Dettagli della policy 1003
Versione della politica 1003
Documento di policy JSON 1003
Ulteriori informazioni 1004
AmazonMechanicalTurkFullAccess 1004
Utilizzo di questa politica 1004
Dettagli della policy 1004
Versione della politica 1005
Documento di policy JSON 1005
Ulteriori informazioni 1005
AmazonMechanicalTurkReadOnly 1005
Utilizzo di questa politica 1006
Dettagli della policy 1006
Versione della politica 1006
Documento di policy JSON 1006
Ulteriori informazioni 1007
AmazonMemoryDBFullAccess 1007
Utilizzo di questa politica 1007
Dettagli della policy 1007
Versione della politica 1007
Documento di policy JSON 1007
Ulteriori informazioni 1008

AmazonMemoryDBReadOnlyAccess 1008
Utilizzo di questa politica 1008
Dettagli della policy 1008
Versione della politica 1009
Documento di policy JSON 1009
Ulteriori informazioni 1009
AmazonMobileAnalyticsFinancialReportAccess 1009
Utilizzo di questa politica 1010
Dettagli della policy 1010
Versione della politica 1010
Documento di policy JSON 1010
Ulteriori informazioni 1011
AmazonMobileAnalyticsFullAccess 1011
Utilizzo di questa politica 1011
Dettagli della policy 1011
Versione della politica 1011
Documento di policy JSON 1011
Ulteriori informazioni 1012
AmazonMobileAnalyticsNon-financialReportAccess 1012
Utilizzo di questa politica 1012
Dettagli della policy 1012
Versione della politica 1012
Documento di policy JSON 1013
Ulteriori informazioni 1013
AmazonMobileAnalyticsWriteOnlyAccess 1013
Utilizzo di questa politica 1013
Dettagli della policy 1013
Versione della politica 1014
Documento di policy JSON 1014
Ulteriori informazioni 1014
AmazonMonitronFullAccess 1014
Utilizzo di questa politica 1015
Dettagli della policy 1015
Versione della politica 1015
Documento di policy JSON 1015
Ulteriori informazioni 1017

AmazonMQApiFullAccess 1017
Utilizzo di questa politica 1017
Dettagli della policy 1017
Versione della politica 1018
Documento di policy JSON 1018
Ulteriori informazioni 1019
AmazonMQApiReadOnlyAccess 1019
Utilizzo di questa politica 1019
Dettagli della policy 1019
Versione della politica 1019
Documento di policy JSON 1020
Ulteriori informazioni 1020
AmazonMQFullAccess 1020
Utilizzo di questa politica 1020
Dettagli della policy 1021
Versione della politica 1021
Documento di policy JSON 1021
Ulteriori informazioni 1022
AmazonMQReadOnlyAccess 1022
Utilizzo di questa politica 1022
Dettagli della policy 1023
Versione della politica 1023
Documento di policy JSON 1023
Ulteriori informazioni 1023
AmazonMQServiceRolePolicy 1024
Utilizzo di questa politica 1024
Dettagli della policy 1024
Versione della politica 1024
Documento di policy JSON 1024
Ulteriori informazioni 1026
AmazonMSKConnectReadOnlyAccess 1026
Utilizzo di questa politica 1026
Dettagli della policy 1026
Versione della politica 1027
Documento di policy JSON 1027
Ulteriori informazioni 1028

AmazonMSKFullAccess 1028
Utilizzo di questa politica 1028
Dettagli della policy 1028
Versione della politica 1029
Documento di policy JSON 1029
Ulteriori informazioni 1032
AmazonMSKReadOnlyAccess 1032
Utilizzo di questa politica 1032
Dettagli della policy 1032
Versione della politica 1032
Documento di policy JSON 1032
Ulteriori informazioni 1033
AmazonMWAAServerlessServiceRolePolicy 1033
Utilizzo di questa politica 1033
Dettagli della policy 1033
Versione della politica 1034
Documento di policy JSON 1034
Ulteriori informazioni 1034
AmazonMWAAServiceRolePolicy 1035
Utilizzo di questa politica 1035
Dettagli della policy 1035
Versione della politica 1035
Documento di policy JSON 1035
Ulteriori informazioni 1038
AmazonNimbleStudio-LaunchProfileWorker 1038
Utilizzo di questa politica 1038
Dettagli della policy 1038
Versione della politica 1038
Documento di policy JSON 1038
Ulteriori informazioni 1039
AmazonNimbleStudio-StudioAdmin 1039
Utilizzo di questa politica 1039
Dettagli della policy 1040
Versione della politica 1040
Documento di policy JSON 1040
Ulteriori informazioni 1042

AmazonNimbleStudio-StudioUser 1042
Utilizzo di questa politica 1042
Dettagli della policy 1042
Versione della politica 1043
Documento di policy JSON 1043
Ulteriori informazioni 1045
AmazonODBFullAccess 1045
Utilizzo di questa politica 1045
Dettagli della policy 1045
Versione della politica 1045
Documento sulla politica JSON 1046
Ulteriori informazioni 1049
AmazonODBServiceRolePolicy 1049
Utilizzo di questa politica 1049
Dettagli della policy 1049
Versione della politica 1049
Documento di policy JSON 1049
Ulteriori informazioni 1051
AmazonOmicsFullAccess 1051
Utilizzo di questa politica 1051
Dettagli della policy 1051
Versione della politica 1052
Documento di policy JSON 1052
Ulteriori informazioni 1053
AmazonOmicsReadOnlyAccess 1053
Utilizzo di questa politica 1053
Dettagli della policy 1053
Versione della politica 1053
Documento di policy JSON 1054
Ulteriori informazioni 1054
AmazonOneEnterpriseFullAccess 1054
Utilizzo di questa politica 1054
Dettagli della policy 1054
Versione della politica 1055
Documento di policy JSON 1055
Ulteriori informazioni 1055

AmazonOneEnterpriseInstallerAccess 1055
Utilizzo di questa politica 1056
Dettagli della policy 1056
Versione della politica 1056
Documento di policy JSON 1056
Ulteriori informazioni 1057
AmazonOneEnterpriseReadOnlyAccess 1057
Utilizzo di questa politica 1057
Dettagli della policy 1057
Versione della politica 1057
Documento di policy JSON 1057
Ulteriori informazioni 1058
AmazonOpenSearchDashboardsServiceRolePolicy 1058
Utilizzo di questa politica 1058
Dettagli della policy 1058
Versione della politica 1059
Documento di policy JSON 1059
Ulteriori informazioni 1059
AmazonOpenSearchDirectQueryGlueCreateAccess 1059
Utilizzo di questa politica 1060
Dettagli della policy 1060
Versione della politica 1060
Documento di policy JSON 1060
Ulteriori informazioni 1061
AmazonOpenSearchIngestionFullAccess 1061
Utilizzo di questa politica 1061
Dettagli della policy 1061
Versione della politica 1061
Documento di policy JSON 1061
Ulteriori informazioni 1062
AmazonOpenSearchIngestionReadOnlyAccess 1063
Utilizzo di questa politica 1063
Dettagli della policy 1063
Versione della politica 1063
Documento di policy JSON 1063
Ulteriori informazioni 1064

AmazonOpenSearchIngestionServiceRolePolicy 1064
Utilizzo di questa politica 1064
Dettagli della policy 1064
Versione della politica 1064
Documento di policy JSON 1065
Ulteriori informazioni 1066
AmazonOpenSearchServerlessServiceRolePolicy 1067
Utilizzo di questa politica 1067
Dettagli della policy 1067
Versione della politica 1067
Documento di policy JSON 1067
Ulteriori informazioni 1068
AmazonOpenSearchServiceCognitoAccess 1068
Utilizzo di questa politica 1068
Dettagli della policy 1068
Versione della politica 1068
Documento di policy JSON 1069
Ulteriori informazioni 1070
AmazonOpenSearchServiceFullAccess 1070
Utilizzo di questa politica 1070
Dettagli della policy 1070
Versione della politica 1070
Documento di policy JSON 1071
Ulteriori informazioni 1071
AmazonOpenSearchServiceReadOnlyAccess 1071
Utilizzo di questa politica 1071
Dettagli della policy 1071
Versione della politica 1072
Documento di policy JSON 1072
Ulteriori informazioni 1072
AmazonOpenSearchServiceRolePolicy 1073
Utilizzo di questa politica 1073
Dettagli della policy 1073
Versione della politica 1073
Documento di policy JSON 1073
Ulteriori informazioni 1078

AmazonPersonalizeFullAccess 1078
Utilizzo di questa politica 1078
Dettagli della policy 1078
Versione della politica 1079
Documento di policy JSON 1079
Ulteriori informazioni 1080
AmazonPollyFullAccess 1080
Utilizzo di questa politica 1080
Dettagli della policy 1080
Versione della politica 1081
Documento di policy JSON 1081
Ulteriori informazioni 1081
AmazonPollyReadOnlyAccess 1081
Utilizzo di questa politica 1082
Dettagli della policy 1082
Versione della politica 1082
Documento di policy JSON 1082
Ulteriori informazioni 1083
AmazonPrometheusConsoleFullAccess 1083
Utilizzo di questa politica 1083
Dettagli della policy 1083
Versione della politica 1083
Documento di policy JSON 1084
Ulteriori informazioni 1085
AmazonPrometheusFullAccess 1085
Utilizzo di questa politica 1085
Dettagli della policy 1085
Versione della politica 1085
Documento di policy JSON 1086
Ulteriori informazioni 1087
AmazonPrometheusQueryAccess 1087
Utilizzo di questa politica 1087
Dettagli della policy 1087
Versione della politica 1087
Documento di policy JSON 1087
Ulteriori informazioni 1088

AmazonPrometheusRemoteWriteAccess 1088
Utilizzo di questa politica 1088
Dettagli della policy 1088
Versione della politica 1089
Documento di policy JSON 1089
Ulteriori informazioni 1089
AmazonPrometheusScraperServiceRolePolicy 1089
Utilizzo di questa politica 1090
Dettagli della policy 1090
Versione della politica 1090
Documento sulla politica JSON 1090
Ulteriori informazioni 1093
AmazonQDeveloperAccess 1093
Utilizzo di questa politica 1093
Dettagli della policy 1093
Versione della politica 1093
Documento di policy JSON 1093
Ulteriori informazioni 1095
AmazonQFullAccess 1095
Utilizzo di questa politica 1095
Dettagli della policy 1095
Versione della politica 1095
Documento di policy JSON 1096
Ulteriori informazioni 1098
AmazonQLDBConsoleFullAccess 1098
Utilizzo di questa politica 1098
Dettagli della policy 1098
Versione della politica 1098
Documento di policy JSON 1098
Ulteriori informazioni 1100
AmazonQLDBFullAccess 1100
Utilizzo di questa politica 1100
Dettagli della policy 1101
Versione della politica 1101
Documento di policy JSON 1101
Ulteriori informazioni 1102

AmazonQLDBReadOnly 1102
Utilizzo di questa politica 1103
Dettagli della policy 1103
Versione della politica 1103
Documento di policy JSON 1103
Ulteriori informazioni 1104
AmazonRDSBetaServiceRolePolicy 1104
Utilizzo di questa politica 1104
Dettagli della policy 1104
Versione della politica 1104
Documento di policy JSON 1105
Ulteriori informazioni 1108
AmazonRDSCustomInstanceProfileRolePolicy 1108
Utilizzo di questa politica 1108
Dettagli della policy 1108
Versione della politica 1108
Documento di policy JSON 1108
Ulteriori informazioni 1116
AmazonRDSCustomPreviewServiceRolePolicy 1116
Utilizzo di questa politica 1116
Dettagli della policy 1116
Versione della politica 1116
Documento di policy JSON 1117
Ulteriori informazioni 1134
AmazonRDSCustomServiceRolePolicy 1134
Utilizzo di questa politica 1134
Dettagli della policy 1134
Versione della politica 1135
Documento di policy JSON 1135
Ulteriori informazioni 1154
AmazonRDSDataFullAccess 1154
Utilizzo di questa politica 1154
Dettagli della policy 1154
Versione della politica 1154
Documento di policy JSON 1155
Ulteriori informazioni 1156

AmazonRDSDirectoryServiceAccess 1156
Utilizzo di questa politica 1156
Dettagli della policy 1156
Versione della politica 1156
Documento di policy JSON 1157
Ulteriori informazioni 1157
AmazonRDSEnhancedMonitoringRole 1157
Utilizzo di questa politica 1157
Dettagli della policy 1158
Versione della politica 1158
Documento di policy JSON 1158
Ulteriori informazioni 1159
AmazonRDSFullAccess 1159
Utilizzo di questa politica 1159
Dettagli della policy 1159
Versione della politica 1159
Documento di policy JSON 1160
Ulteriori informazioni 1162
AmazonRDSPerformanceInsightsFullAccess 1162
Utilizzo di questa politica 1162
Dettagli della policy 1162
Versione della politica 1162
Documento sulla politica JSON 1162
Ulteriori informazioni 1164
AmazonRDSPerformanceInsightsReadOnly 1164
Utilizzo di questa politica 1164
Dettagli della policy 1165
Versione della politica 1165
Documento sulla politica JSON 1165
Ulteriori informazioni 1167
AmazonRDSPreviewServiceRolePolicy 1167
Utilizzo di questa politica 1168
Dettagli della policy 1168
Versione della politica 1168
Documento di policy JSON 1168
Ulteriori informazioni 1171

AmazonRDSReadOnlyAccess 1171
Utilizzo di questa politica 1171
Dettagli della policy 1171
Versione della politica 1172
Documento di policy JSON 1172
Ulteriori informazioni 1173
AmazonRDSServiceRolePolicy 1173
Utilizzo di questa politica 1174
Dettagli della policy 1174
Versione della politica 1174
Documento di policy JSON 1174
Ulteriori informazioni 1178
AmazonRedshiftAllCommandsFullAccess 1178
Utilizzo di questa politica 1178
Dettagli della policy 1178
Versione della politica 1179
Documento di policy JSON 1179
Ulteriori informazioni 1184
AmazonRedshiftDataFullAccess 1184
Utilizzo di questa politica 1184
Dettagli della policy 1184
Versione della politica 1185
Documento di policy JSON 1185
Ulteriori informazioni 1187
AmazonRedshiftFederatedAuthorization 1187
Utilizzo di questa politica 1187
Dettagli della policy 1187
Versione della politica 1187
Documento di policy JSON 1188
Ulteriori informazioni 1189
AmazonRedshiftFullAccess 1189
Utilizzo di questa politica 1189
Dettagli della policy 1189
Versione della politica 1189
Documento di policy JSON 1190
Ulteriori informazioni 1192

AmazonRedshiftQueryEditor 1192
Utilizzo di questa politica 1192
Dettagli della policy 1192
Versione della politica 1192
Documento di policy JSON 1192
Ulteriori informazioni 1194
AmazonRedshiftQueryEditorV2FullAccess 1195
Utilizzo di questa politica 1195
Dettagli della policy 1195
Versione della politica 1195
Documento di policy JSON 1195
Ulteriori informazioni 1197
AmazonRedshiftQueryEditorV2NoSharing 1197
Utilizzo di questa politica 1197
Dettagli della policy 1197
Versione della politica 1197
Documento di policy JSON 1198
Ulteriori informazioni 1201
AmazonRedshiftQueryEditorV2ReadSharing 1201
Utilizzo di questa politica 1202
Dettagli della policy 1202
Versione della politica 1202
Documento di policy JSON 1202
Ulteriori informazioni 1207
AmazonRedshiftQueryEditorV2ReadWriteSharing 1207
Utilizzo di questa politica 1208
Dettagli della policy 1208
Versione della politica 1208
Documento di policy JSON 1208
Ulteriori informazioni 1213
AmazonRedshiftReadOnlyAccess 1213
Utilizzo di questa politica 1213
Dettagli della policy 1213
Versione della politica 1214
Documento di policy JSON 1214
Ulteriori informazioni 1215

AmazonRedshiftServiceLinkedRolePolicy 1215
Utilizzo di questa politica 1215
Dettagli della policy 1215
Versione della politica 1215
Documento di policy JSON 1215
Ulteriori informazioni 1222
AmazonRekognitionCustomLabelsFullAccess 1222
Utilizzo di questa politica 1222
Dettagli della policy 1222
Versione della politica 1222
Documento di policy JSON 1223
Ulteriori informazioni 1224
AmazonRekognitionFullAccess 1224
Utilizzo di questa politica 1224
Dettagli della policy 1224
Versione della politica 1224
Documento di policy JSON 1225
Ulteriori informazioni 1225
AmazonRekognitionReadOnlyAccess 1225
Utilizzo di questa politica 1225
Dettagli della policy 1225
Versione della politica 1226
Documento di policy JSON 1226
Ulteriori informazioni 1227
AmazonRekognitionServiceRole 1227
Utilizzo di questa politica 1227
Dettagli della policy 1228
Versione della politica 1228
Documento di policy JSON 1228
Ulteriori informazioni 1229
AmazonRoute53AutoNamingFullAccess 1229
Utilizzo di questa politica 1229
Dettagli della policy 1229
Versione della politica 1229
Documento di policy JSON 1230
Ulteriori informazioni 1230

AmazonRoute53AutoNamingReadOnlyAccess 1230
Utilizzo di questa politica 1231
Dettagli della policy 1231
Versione della politica 1231
Documento di policy JSON 1231
Ulteriori informazioni 1232
AmazonRoute53AutoNamingRegistrantAccess 1232
Utilizzo di questa politica 1232
Dettagli della policy 1232
Versione della politica 1232
Documento di policy JSON 1232
Ulteriori informazioni 1233
AmazonRoute53DomainsFullAccess 1233
Utilizzo di questa politica 1234
Dettagli della policy 1234
Versione della politica 1234
Documento di policy JSON 1234
Ulteriori informazioni 1235
AmazonRoute53DomainsReadOnlyAccess 1235
Utilizzo di questa politica 1235
Dettagli della policy 1235
Versione della politica 1235
Documento di policy JSON 1235
Ulteriori informazioni 1236
AmazonRoute53FullAccess 1236
Utilizzo di questa politica 1236
Dettagli della policy 1236
Versione della politica 1237
Documento di policy JSON 1237
Ulteriori informazioni 1238
AmazonRoute53GlobalResolverFullAccess 1238
Utilizzo di questa politica 1238
Dettagli della policy 1238
Versione della politica 1238
Documento di policy JSON 1239
Ulteriori informazioni 1240

AmazonRoute53GlobalResolverReadOnlyAccess 1240
Utilizzo di questa politica 1241
Dettagli della policy 1241
Versione della politica 1241
Documento di policy JSON 1241
Ulteriori informazioni 1242
AmazonRoute53ProfilesFullAccess 1242
Utilizzo di questa politica 1242
Dettagli della policy 1242
Versione della politica 1243
Documento di policy JSON 1243
Ulteriori informazioni 1244
AmazonRoute53ProfilesReadOnlyAccess 1244
Utilizzo di questa politica 1244
Dettagli della policy 1244
Versione della politica 1244
Documento di policy JSON 1245
Ulteriori informazioni 1245
AmazonRoute53ReadOnlyAccess 1246
Utilizzo di questa politica 1246
Dettagli della policy 1246
Versione della politica 1246
Documento di policy JSON 1246
Ulteriori informazioni 1247
AmazonRoute53RecoveryClusterFullAccess 1247
Utilizzo di questa politica 1247
Dettagli della policy 1247
Versione della politica 1247
Documento di policy JSON 1248
Ulteriori informazioni 1248
AmazonRoute53RecoveryClusterReadOnlyAccess 1248
Utilizzo di questa politica 1248
Dettagli della policy 1248
Versione della politica 1249
Documento di policy JSON 1249
Ulteriori informazioni 1249

AmazonRoute53RecoveryControlConfigFullAccess 1249
Utilizzo di questa politica 1250
Dettagli della policy 1250
Versione della politica 1250
Documento di policy JSON 1250
Ulteriori informazioni 1250
AmazonRoute53RecoveryControlConfigReadOnlyAccess 1251
Utilizzo di questa politica 1251
Dettagli della policy 1251
Versione della politica 1251
Documento di policy JSON 1251
Ulteriori informazioni 1252
AmazonRoute53RecoveryReadinessFullAccess 1252
Utilizzo di questa politica 1252
Dettagli della policy 1252
Versione della politica 1253
Documento di policy JSON 1253
Ulteriori informazioni 1253
AmazonRoute53RecoveryReadinessReadOnlyAccess 1253
Utilizzo di questa politica 1254
Dettagli della policy 1254
Versione della politica 1254
Documento di policy JSON 1254
Ulteriori informazioni 1255
AmazonRoute53ResolverFullAccess 1255
Utilizzo di questa politica 1255
Dettagli della policy 1255
Versione della politica 1256
Documento di policy JSON 1256
Ulteriori informazioni 1256
AmazonRoute53ResolverReadOnlyAccess 1257
Utilizzo di questa politica 1257
Dettagli della policy 1257
Versione della politica 1257
Documento di policy JSON 1257
Ulteriori informazioni 1258

AmazonS3ExpressFullAccess 1258
Utilizzo di questa politica 1258
Dettagli della policy 1258
Versione della politica 1259
Documento di policy JSON 1259
Ulteriori informazioni 1259
AmazonS3ExpressReadOnlyAccess 1259
Utilizzo di questa politica 1259
Dettagli della policy 1260
Versione della politica 1260
Documento di policy JSON 1260
Ulteriori informazioni 1261
AmazonS3FilesClientFullAccess 1261
Utilizzo di questa politica 1261
Dettagli della policy 1261
Versione della politica 1261
Documento di policy JSON 1262
Ulteriori informazioni 1262
AmazonS3FilesClientReadOnlyAccess 1262
Utilizzo di questa politica 1262
Dettagli della policy 1263
Versione della politica 1263
Documento di policy JSON 1263
Ulteriori informazioni 1263
AmazonS3FilesClientReadWriteAccess 1264
Utilizzo di questa politica 1264
Dettagli della policy 1264
Versione della politica 1264
Documento di policy JSON 1264
Ulteriori informazioni 1265
AmazonS3FilesCSIDriverPolicy 1265
Utilizzo di questa politica 1265
Dettagli della policy 1265
Versione della politica 1265
Documento di policy JSON 1266
Ulteriori informazioni 1267

AmazonS3FilesFullAccess 1267
Utilizzo di questa politica 1267
Dettagli della policy 1267
Versione della politica 1268
Documento di policy JSON 1268
Ulteriori informazioni 1270
AmazonS3FilesReadOnlyAccess 1270
Utilizzo di questa politica 1270
Dettagli della policy 1270
Versione della politica 1270
Documento di policy JSON 1271
Ulteriori informazioni 1271
AmazonS3FullAccess 1272
Utilizzo di questa politica 1272
Dettagli della policy 1272
Versione della politica 1272
Documento di policy JSON 1272
Ulteriori informazioni 1273
AmazonS3ObjectLambdaExecutionRolePolicy 1273
Utilizzo di questa politica 1273
Dettagli della policy 1273
Versione della politica 1273
Documento di policy JSON 1274
Ulteriori informazioni 1274
AmazonS3OutpostsFullAccess 1274
Utilizzo di questa politica 1274
Dettagli della policy 1274
Versione della politica 1275
Documento di policy JSON 1275
Ulteriori informazioni 1276
AmazonS3OutpostsReadOnlyAccess 1276
Utilizzo di questa politica 1276
Dettagli della policy 1276
Versione della politica 1277
Documento di policy JSON 1277
Ulteriori informazioni 1278

AmazonS3ReadOnlyAccess 1278
Utilizzo di questa politica 1278
Dettagli della policy 1278
Versione della politica 1278
Documento di policy JSON 1279
Ulteriori informazioni 1279
AmazonS3TablesFullAccess 1279
Utilizzo di questa politica 1279
Dettagli della policy 1280
Versione della politica 1280
Documento di policy JSON 1280
Ulteriori informazioni 1281
AmazonS3TablesLakeFormationServiceRole 1281
Utilizzo di questa politica 1281
Dettagli della policy 1281
Versione della politica 1281
Documento di policy JSON 1282
Ulteriori informazioni 1284
AmazonS3TablesReadOnlyAccess 1284
Utilizzo di questa politica 1284
Dettagli della policy 1284
Versione della politica 1284
Documento di policy JSON 1285
Ulteriori informazioni 1285
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 1285
Utilizzo di questa politica 1286
Dettagli della policy 1286
Versione della politica 1286
Documento di policy JSON 1286
Ulteriori informazioni 1297
AmazonSageMakerCanvasAIServicesAccess 1298
Utilizzo di questa politica 1298
Dettagli della policy 1298
Versione della politica 1298
Documento di policy JSON 1298
Ulteriori informazioni 1301

AmazonSageMakerCanvasBedrockAccess 1302
Utilizzo di questa politica 1302
Dettagli della policy 1302
Versione della politica 1302
Documento di policy JSON 1302
Ulteriori informazioni 1303
AmazonSageMakerCanvasDataPrepFullAccess 1303
Utilizzo di questa politica 1303
Dettagli della policy 1304
Versione della politica 1304
Documento di policy JSON 1304
Ulteriori informazioni 1313
AmazonSageMakerCanvasDirectDeployAccess 1314
Utilizzo di questa politica 1314
Dettagli della policy 1314
Versione della politica 1314
Documento di policy JSON 1314
Ulteriori informazioni 1315
AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy 1315
Utilizzo di questa politica 1315
Dettagli della policy 1316
Versione della politica 1316
Documento di policy JSON 1316
Ulteriori informazioni 1317
AmazonSageMakerCanvasForecastAccess 1318
Utilizzo di questa politica 1318
Dettagli della policy 1318
Versione della politica 1318
Documento di policy JSON 1318
Ulteriori informazioni 1319
AmazonSageMakerCanvasFullAccess 1319
Utilizzo di questa politica 1319
Dettagli della policy 1319
Versione della politica 1320
Documento di policy JSON 1320
Ulteriori informazioni 1332

AmazonSageMakerCanvasSMDataScienceAssistantAccess 1332
Utilizzo di questa politica 1332
Dettagli della policy 1332
Versione della politica 1333
Documento di policy JSON 1333
Ulteriori informazioni 1334
AmazonSageMakerCapacityReservationServiceRolePolicy 1334
Utilizzo di questa politica 1334
Dettagli della policy 1334
Versione della politica 1334
Documento di policy JSON 1335
Ulteriori informazioni 1335
AmazonSageMakerClusterInstanceRolePolicy 1335
Utilizzo di questa politica 1336
Dettagli della policy 1336
Versione della politica 1336
Documento di policy JSON 1336
Ulteriori informazioni 1338
AmazonSageMakerCoreServiceRolePolicy 1338
Utilizzo di questa politica 1338
Dettagli della policy 1338
Versione della politica 1338
Documento di policy JSON 1339
Ulteriori informazioni 1340
AmazonSageMakerEdgeDeviceFleetPolicy 1340
Utilizzo di questa politica 1340
Dettagli della policy 1340
Versione della politica 1340
Documento di policy JSON 1340
Ulteriori informazioni 1342
AmazonSageMakerFeatureStoreAccess 1342
Utilizzo di questa politica 1343
Dettagli della policy 1343
Versione della politica 1343
Documento di policy JSON 1343
Ulteriori informazioni 1344

AmazonSageMakerFullAccess 1344
Utilizzo di questa politica 1345
Dettagli della policy 1345
Versione della politica 1345
Documento di policy JSON 1345
Ulteriori informazioni 1361
AmazonSageMakerGeospatialExecutionRole 1362
Utilizzo di questa politica 1362
Dettagli della policy 1362
Versione della politica 1362
Documento di policy JSON 1362
Ulteriori informazioni 1363
AmazonSageMakerGeospatialFullAccess 1363
Utilizzo di questa politica 1363
Dettagli della policy 1364
Versione della politica 1364
Documento di policy JSON 1364
Ulteriori informazioni 1365
AmazonSageMakerGroundTruthExecution 1365
Utilizzo di questa politica 1365
Dettagli della policy 1365
Versione della politica 1365
Documento di policy JSON 1366
Ulteriori informazioni 1369
AmazonSageMakerHyperPodGatedModelAccess 1369
Utilizzo di questa politica 1369
Dettagli della policy 1370
Versione della politica 1370
Documento di policy JSON 1370
Ulteriori informazioni 1371
AmazonSageMakerHyperPodInferenceAccess 1371
Utilizzo di questa politica 1371
Dettagli della policy 1371
Versione della politica 1371
Documento sulla politica JSON 1372
Ulteriori informazioni 1380

AmazonSageMakerHyperPodObservabilityAdminAccess 1381
Utilizzo di questa politica 1381
Dettagli della policy 1381
Versione della politica 1381
Documento di policy JSON 1381
Ulteriori informazioni 1388
AmazonSageMakerHyperPodServiceRolePolicy 1388
Utilizzo di questa politica 1388
Dettagli della policy 1388
Versione della politica 1388
Documento di policy JSON 1389
Ulteriori informazioni 1390
AmazonSageMakerHyperPodTrainingOperatorAccess 1390
Utilizzo di questa politica 1390
Dettagli della policy 1390
Versione della politica 1390
Documento di policy JSON 1391
Ulteriori informazioni 1391
AmazonSageMakerInferenceServiceRolePolicy 1391
Utilizzo di questa politica 1391
Dettagli della policy 1392
Versione della politica 1392
Documento sulla politica JSON 1392
Ulteriori informazioni 1395
AmazonSageMakerJobFullAccess 1395
Utilizzo di questa politica 1395
Dettagli della policy 1395
Versione della politica 1395
Documento di policy JSON 1396
Ulteriori informazioni 1400
AmazonSageMakerJobRuntimeAccess 1401
Utilizzo di questa politica 1401
Dettagli della policy 1401
Versione della politica 1401
Documento di policy JSON 1401
Ulteriori informazioni 1402

AmazonSageMakerMechanicalTurkAccess 1402
Utilizzo di questa politica 1403
Dettagli della policy 1403
Versione della politica 1403
Documento di policy JSON 1403
Ulteriori informazioni 1403
AmazonSageMakerModelCustomizationCoreAccess 1404
Utilizzo di questa politica 1404
Dettagli della policy 1404
Versione della politica 1404
Documento sulla politica JSON 1404
Ulteriori informazioni 1416
AmazonSageMakerModelGovernanceUseAccess 1416
Utilizzo di questa politica 1416
Dettagli della policy 1417
Versione della politica 1417
Documento di policy JSON 1417
Ulteriori informazioni 1419
AmazonSageMakerModelRegistryFullAccess 1419
Utilizzo di questa politica 1419
Dettagli della policy 1419
Versione della politica 1420
Documento di policy JSON 1420
Ulteriori informazioni 1423
AmazonSageMakerNotebooksServiceRolePolicy 1424
Utilizzo di questa politica 1424
Dettagli della policy 1424
Versione della politica 1424
Documento di policy JSON 1424
Ulteriori informazioni 1429
AmazonSageMakerPartnerAppsFullAccess 1430
Utilizzo di questa politica 1430
Dettagli della policy 1430
Versione della politica 1430
Documento di policy JSON 1430
Ulteriori informazioni 1431

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 1431
Utilizzo di questa politica 1431
Dettagli della policy 1432
Versione della politica 1432
Documento di policy JSON 1432
Ulteriori informazioni 1433
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 1433
Utilizzo di questa politica 1433
Dettagli della policy 1433
Versione della politica 1434
Documento di policy JSON 1434
Ulteriori informazioni 1437
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 1438
Utilizzo di questa politica 1438
Dettagli della policy 1438
Versione della politica 1438
Documento di policy JSON 1438
Ulteriori informazioni 1439
AmazonSageMakerPipelinesIntegrations 1439
Utilizzo di questa politica 1439
Dettagli della policy 1439
Versione della politica 1440
Documento di policy JSON 1440
Ulteriori informazioni 1442
AmazonSageMakerQuickSightVPCPolicy 1442
Utilizzo di questa politica 1442
Dettagli della policy 1442
Versione della politica 1442
Documento di policy JSON 1443
Ulteriori informazioni 1444
AmazonSageMakerReadOnly 1444
Utilizzo di questa politica 1444
Dettagli della policy 1445
Versione della politica 1445
Documento di policy JSON 1445
Ulteriori informazioni 1446

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 1446
Utilizzo di questa politica 1447
Dettagli della policy 1447
Versione della politica 1447
Documento di policy JSON 1447
Ulteriori informazioni 1448
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 1448
Utilizzo di questa politica 1448
Dettagli della policy 1448
Versione della politica 1449
Documento di policy JSON 1449
Ulteriori informazioni 1456
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 1456
Utilizzo di questa politica 1456
Dettagli della policy 1456
Versione della politica 1456
Documento di policy JSON 1457
Ulteriori informazioni 1467
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 1467
Utilizzo di questa politica 1467
Dettagli della policy 1467
Versione della politica 1468
Documento di policy JSON 1468
Ulteriori informazioni 1471
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 1471
Utilizzo di questa politica 1471
Dettagli della policy 1471
Versione della politica 1471
Documento di policy JSON 1472
Ulteriori informazioni 1472
AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 1472
Utilizzo di questa politica 1472
Dettagli della policy 1472
Versione della politica 1473
Documento di policy JSON 1473
Ulteriori informazioni 1473

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 1474
Utilizzo di questa politica 1474
Dettagli della policy 1474
Versione della politica 1474
Documento di policy JSON 1474
Ulteriori informazioni 1476
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 1477
Utilizzo di questa politica 1477
Dettagli della policy 1477
Versione della politica 1477
Documento di policy JSON 1477
Ulteriori informazioni 1487
AmazonSageMakerSpacesControllerPolicy 1488
Utilizzo di questa politica 1488
Dettagli della policy 1488
Versione della politica 1488
Documento di policy JSON 1488
Ulteriori informazioni 1493
AmazonSageMakerSpacesRouterPolicy 1493
Utilizzo di questa politica 1493
Dettagli della policy 1493
Versione della politica 1494
Documento di policy JSON 1494
Ulteriori informazioni 1495
AmazonSageMakerTrainingPlanCreateAccess 1495
Utilizzo di questa politica 1495
Dettagli della policy 1495
Versione della politica 1495
Documento di policy JSON 1496
Ulteriori informazioni 1497
AmazonSecurityLakeAdministrator 1497
Utilizzo di questa politica 1497
Dettagli della policy 1498
Versione della politica 1498
Documento di policy JSON 1498
Ulteriori informazioni 1509

AmazonSecurityLakeMetastoreManager 1509
Utilizzo di questa politica 1509
Dettagli della policy 1510
Versione della politica 1510
Documento di policy JSON 1510
Ulteriori informazioni 1512
AmazonSecurityLakePermissionsBoundary 1512
Utilizzo di questa politica 1513
Dettagli della policy 1513
Versione della politica 1513
Documento di policy JSON 1513
Ulteriori informazioni 1516
AmazonSESFullAccess 1516
Utilizzo di questa politica 1517
Dettagli della policy 1517
Versione della politica 1517
Documento di policy JSON 1517
Ulteriori informazioni 1517
AmazonSESReadOnlyAccess 1518
Utilizzo di questa politica 1518
Dettagli della policy 1518
Versione della politica 1518
Documento di policy JSON 1518
Ulteriori informazioni 1519
AmazonSESServiceRolePolicy 1519
Utilizzo di questa politica 1519
Dettagli della policy 1519
Versione della politica 1519
Documento di policy JSON 1520
Ulteriori informazioni 1520
AmazonSNSFullAccess 1520
Utilizzo di questa politica 1520
Dettagli della policy 1521
Versione della politica 1521
Documento di policy JSON 1521
Ulteriori informazioni 1522

AmazonSNSReadOnlyAccess 1522
Utilizzo di questa politica 1522
Dettagli della policy 1522
Versione della politica 1523
Documento di policy JSON 1523
Ulteriori informazioni 1524
AmazonSNSRole 1524
Utilizzo di questa politica 1524
Dettagli della policy 1524
Versione della politica 1524
Documento di policy JSON 1525
Ulteriori informazioni 1525
AmazonSQSFullAccess 1525
Utilizzo di questa politica 1525
Dettagli della policy 1526
Versione della politica 1526
Documento di policy JSON 1526
Ulteriori informazioni 1526
AmazonSQSReadOnlyAccess 1527
Utilizzo di questa politica 1527
Dettagli della policy 1527
Versione della politica 1527
Documento di policy JSON 1527
Ulteriori informazioni 1528
AmazonSSMAutomationApproverAccess 1528
Utilizzo di questa politica 1528
Dettagli della policy 1528
Versione della politica 1528
Documento di policy JSON 1529
Ulteriori informazioni 1529
AmazonSSMAutomationRole 1529
Utilizzo di questa politica 1529
Dettagli della policy 1530
Versione della politica 1530
Documento di policy JSON 1530
Ulteriori informazioni 1532

AmazonSSMDirectoryServiceAccess 1532
Utilizzo di questa politica 1532
Dettagli della policy 1532
Versione della politica 1532
Documento di policy JSON 1533
Ulteriori informazioni 1533
AmazonSSMFullAccess 1533
Utilizzo di questa politica 1533
Dettagli della policy 1533
Versione della politica 1534
Documento di policy JSON 1534
Ulteriori informazioni 1535
AmazonSSMMaintenanceWindowRole 1535
Utilizzo di questa politica 1535
Dettagli della policy 1535
Versione della politica 1536
Documento di policy JSON 1536
Ulteriori informazioni 1537
AmazonSSMManagedEC2InstanceDefaultPolicy 1537
Utilizzo di questa politica 1538
Dettagli della policy 1538
Versione della politica 1538
Documento di policy JSON 1538
Ulteriori informazioni 1539
AmazonSSMManagedInstanceCore 1540
Utilizzo di questa politica 1540
Dettagli della policy 1540
Versione della politica 1540
Documento di policy JSON 1540
Ulteriori informazioni 1541
AmazonSSMPatchAssociation 1542
Utilizzo di questa politica 1542
Dettagli della policy 1542
Versione della politica 1542
Documento di policy JSON 1542
Ulteriori informazioni 1543

AmazonSSMReadOnlyAccess 1543
Utilizzo di questa politica 1543
Dettagli della policy 1543
Versione della politica 1544
Documento di policy JSON 1544
Ulteriori informazioni 1544
AmazonSSMServiceRolePolicy 1544
Utilizzo di questa politica 1545
Dettagli della policy 1545
Versione della politica 1545
Documento di policy JSON 1545
Ulteriori informazioni 1551
AmazonSumerianFullAccess 1551
Utilizzo di questa politica 1551
Dettagli della policy 1551
Versione della politica 1551
Documento di policy JSON 1551
Ulteriori informazioni 1552
AmazonTextractFullAccess 1552
Utilizzo di questa politica 1552
Dettagli della policy 1552
Versione della politica 1552
Documento di policy JSON 1553
Ulteriori informazioni 1553
AmazonTextractServiceRole 1553
Utilizzo di questa politica 1553
Dettagli della policy 1553
Versione della politica 1554
Documento di policy JSON 1554
Ulteriori informazioni 1554
AmazonTimestreamConsoleFullAccess 1554
Utilizzo di questa politica 1555
Dettagli della policy 1555
Versione della politica 1555
Documento di policy JSON 1555
Ulteriori informazioni 1558

AmazonTimestreamFullAccess 1558
Utilizzo di questa politica 1558
Dettagli della policy 1558
Versione della politica 1559
Documento di policy JSON 1559
Ulteriori informazioni 1560
AmazonTimestreamInfluxDBFullAccess 1560
Utilizzo di questa politica 1560
Dettagli della policy 1560
Versione della politica 1561
Documento sulla politica JSON 1561
Ulteriori informazioni 1563
AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess 1564
Utilizzo di questa politica 1564
Dettagli della policy 1564
Versione della politica 1564
Documento sulla politica JSON 1564
Ulteriori informazioni 1567
AmazonTimestreamInfluxDBServiceRolePolicy 1567
Utilizzo di questa politica 1567
Dettagli della policy 1567
Versione della politica 1567
Documento sulla politica JSON 1568
Ulteriori informazioni 1571
AmazonTimestreamReadOnlyAccess 1571
Utilizzo di questa politica 1571
Dettagli della policy 1571
Versione della politica 1571
Documento di policy JSON 1572
Ulteriori informazioni 1572
AmazonTranscribeFullAccess 1573
Utilizzo di questa politica 1573
Dettagli della policy 1573
Versione della politica 1573
Documento di policy JSON 1573
Ulteriori informazioni 1574

AmazonTranscribeReadOnlyAccess 1574
Utilizzo di questa politica 1574
Dettagli della policy 1574
Versione della politica 1574
Documento di policy JSON 1575
Ulteriori informazioni 1575
AmazonVerifiedPermissionsFullAccess 1575
Utilizzo di questa politica 1575
Dettagli della policy 1576
Versione della politica 1576
Documento di policy JSON 1576
Ulteriori informazioni 1577
AmazonVerifiedPermissionsReadOnlyAccess 1577
Utilizzo di questa politica 1577
Dettagli della policy 1577
Versione della politica 1577
Documento di policy JSON 1578
Ulteriori informazioni 1578
AmazonVPCCrossAccountNetworkInterfaceOperations 1579
Utilizzo di questa politica 1579
Dettagli della policy 1579
Versione della politica 1579
Documento di policy JSON 1579
Ulteriori informazioni 1581
AmazonVPCFullAccess 1581
Utilizzo di questa politica 1581
Dettagli della policy 1581
Versione della politica 1581
Documento di policy JSON 1582
Ulteriori informazioni 1585
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 1586
Utilizzo di questa politica 1586
Dettagli della policy 1586
Versione della politica 1586
Documento di policy JSON 1586
Ulteriori informazioni 1590

AmazonVPCReachabilityAnalyzerFullAccessPolicy 1590
Utilizzo di questa politica 1590
Dettagli della policy 1590
Versione della politica 1590
Documento di policy JSON 1591
Ulteriori informazioni 1594
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 1594
Utilizzo di questa politica 1594
Dettagli della policy 1594
Versione della politica 1594
Documento di policy JSON 1595
Ulteriori informazioni 1595
AmazonVPCReadOnlyAccess 1595
Utilizzo di questa politica 1595
Dettagli della policy 1596
Versione della politica 1596
Documento di policy JSON 1596
Ulteriori informazioni 1597
AmazonWorkDocsFullAccess 1597
Utilizzo di questa politica 1598
Dettagli della policy 1598
Versione della politica 1598
Documento di policy JSON 1598
Ulteriori informazioni 1599
AmazonWorkDocsReadOnlyAccess 1599
Utilizzo di questa politica 1599
Dettagli della policy 1599
Versione della politica 1599
Documento di policy JSON 1599
Ulteriori informazioni 1600
AmazonWorkMailEventsServiceRolePolicy 1600
Utilizzo di questa politica 1600
Dettagli della policy 1600
Versione della politica 1601
Documento di policy JSON 1601
Ulteriori informazioni 1601

AmazonWorkMailFullAccess 1601
Utilizzo di questa politica 1602
Dettagli della policy 1602
Versione della politica 1602
Documento di policy JSON 1602
Ulteriori informazioni 1604
AmazonWorkMailMessageFlowFullAccess 1604
Utilizzo di questa politica 1604
Dettagli della policy 1604
Versione della politica 1605
Documento di policy JSON 1605
Ulteriori informazioni 1605
AmazonWorkMailMessageFlowReadOnlyAccess 1605
Utilizzo di questa politica 1606
Dettagli della policy 1606
Versione della politica 1606
Documento di policy JSON 1606
Ulteriori informazioni 1607
AmazonWorkMailReadOnlyAccess 1607
Utilizzo di questa politica 1607
Dettagli della policy 1607
Versione della politica 1607
Documento di policy JSON 1607
Ulteriori informazioni 1608
AmazonWorkSpacesAdmin 1608
Utilizzo di questa politica 1608
Dettagli della policy 1608
Versione della politica 1609
Documento di policy JSON 1609
Ulteriori informazioni 1610
AmazonWorkSpacesApplicationManagerAdminAccess 1610
Utilizzo di questa politica 1610
Dettagli della policy 1610
Versione della politica 1611
Documento di policy JSON 1611
Ulteriori informazioni 1611

AmazonWorkspacesPCAAccess 1611
Utilizzo di questa politica 1612
Dettagli della policy 1612
Versione della politica 1612
Documento di policy JSON 1612
Ulteriori informazioni 1613
AmazonWorkSpacesPoolServiceAccess 1613
Utilizzo di questa politica 1613
Dettagli della policy 1613
Versione della politica 1613
Documento di policy JSON 1614
Ulteriori informazioni 1615
AmazonWorkSpacesSecureBrowserReadOnly 1615
Utilizzo di questa politica 1615
Dettagli della policy 1615
Versione della politica 1615
Documento di policy JSON 1616
Ulteriori informazioni 1617
AmazonWorkSpacesSelfServiceAccess 1617
Utilizzo di questa politica 1617
Dettagli della policy 1617
Versione della politica 1617
Documento di policy JSON 1618
Ulteriori informazioni 1618
AmazonWorkSpacesServiceAccess 1618
Utilizzo di questa politica 1618
Dettagli della policy 1619
Versione della politica 1619
Documento di policy JSON 1619
Ulteriori informazioni 1619
AmazonWorkSpacesThinClientFullAccess 1620
Utilizzo di questa politica 1620
Dettagli della policy 1620
Versione della politica 1620
Documento di policy JSON 1620
Ulteriori informazioni 1622

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 1622
Utilizzo di questa politica 1622
Dettagli della policy 1622
Versione della politica 1622
Documento di policy JSON 1623
Ulteriori informazioni 1623
AmazonWorkSpacesThinClientReadOnlyAccess 1623
Utilizzo di questa politica 1623
Dettagli della policy 1624
Versione della politica 1624
Documento di policy JSON 1624
Ulteriori informazioni 1625
AmazonWorkSpacesWebReadOnly 1625
Utilizzo di questa politica 1626
Dettagli della policy 1626
Versione della politica 1626
Documento di policy JSON 1626
Ulteriori informazioni 1627
AmazonWorkSpacesWebServiceRolePolicy 1627
Utilizzo di questa politica 1627
Dettagli della policy 1628
Versione della politica 1628
Documento di policy JSON 1628
Ulteriori informazioni 1630
AmazonZocaloFullAccess 1630
Utilizzo di questa politica 1631
Dettagli della policy 1631
Versione della politica 1631
Documento di policy JSON 1631
Ulteriori informazioni 1632
AmazonZocaloReadOnlyAccess 1632
Utilizzo di questa politica 1632
Dettagli della policy 1632
Versione della politica 1632
Documento di policy JSON 1633
Ulteriori informazioni 1633

AmplifyBackendDeployFullAccess 1633
Utilizzo di questa politica 1634
Dettagli della policy 1634
Versione della politica 1634
Documento di policy JSON 1634
Ulteriori informazioni 1638
AnthropicFullAccess 1639
Utilizzo di questa politica 1639
Dettagli della policy 1639
Versione della politica 1639
Documento di policy JSON 1639
Ulteriori informazioni 1641
AnthropicInferenceAccess 1641
Utilizzo di questa politica 1641
Dettagli della policy 1641
Versione della politica 1642
Documento di policy JSON 1642
Ulteriori informazioni 1643
AnthropicLimitedAccess 1643
Utilizzo di questa politica 1643
Dettagli della policy 1643
Versione della politica 1644
Documento di policy JSON 1644
Ulteriori informazioni 1646
AnthropicReadOnlyAccess 1646
Utilizzo di questa politica 1646
Dettagli della policy 1647
Versione della politica 1647
Documento di policy JSON 1647
Ulteriori informazioni 1648
AnthropicSelfHostedEnvironmentAccess 1648
Utilizzo di questa politica 1649
Dettagli della policy 1649
Versione della politica 1649
Documento di policy JSON 1649
Ulteriori informazioni 1650

APIGatewayServiceRolePolicy 1650
Utilizzo di questa politica 1650
Dettagli della policy 1650
Versione della politica 1650
Documento di policy JSON 1651
Ulteriori informazioni 1653
AppIntegrationsServiceLinkedRolePolicy 1653
Utilizzo di questa politica 1653
Dettagli della policy 1653
Versione della politica 1654
Documento di policy JSON 1654
Ulteriori informazioni 1655
ApplicationAutoScalingForAmazonAppStreamAccess 1655
Utilizzo di questa politica 1656
Dettagli della policy 1656
Versione della politica 1656
Documento di policy JSON 1656
Ulteriori informazioni 1657
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 1657
Utilizzo di questa politica 1657
Dettagli della policy 1657
Versione della politica 1658
Documento di policy JSON 1658
Ulteriori informazioni 1660
AppRunnerNetworkingServiceRolePolicy 1660
Utilizzo di questa politica 1660
Dettagli della policy 1660
Versione della politica 1660
Documento di policy JSON 1661
Ulteriori informazioni 1662
AppRunnerServiceRolePolicy 1662
Utilizzo di questa politica 1662
Dettagli della policy 1662
Versione della politica 1662
Documento di policy JSON 1663
Ulteriori informazioni 1664

AppStudioServiceRolePolicy 1664
Utilizzo di questa politica 1664
Dettagli della policy 1664
Versione della politica 1664
Documento di policy JSON 1664
Ulteriori informazioni 1667
AuroraDsqlServiceLinkedRolePolicy 1667
Utilizzo di questa politica 1667
Dettagli della policy 1667
Versione della politica 1667
Documento di policy JSON 1667
Ulteriori informazioni 1668
AutoScalingConsoleFullAccess 1668
Utilizzo di questa politica 1668
Dettagli della policy 1668
Versione della politica 1669
Documento di policy JSON 1669
Ulteriori informazioni 1671
AutoScalingConsoleReadOnlyAccess 1671
Utilizzo di questa politica 1671
Dettagli della policy 1671
Versione della politica 1671
Documento di policy JSON 1671
Ulteriori informazioni 1672
AutoScalingFullAccess 1673
Utilizzo di questa politica 1673
Dettagli della policy 1673
Versione della politica 1673
Documento di policy JSON 1673
Ulteriori informazioni 1675
AutoScalingNotificationAccessRole 1675
Utilizzo di questa politica 1675
Dettagli della policy 1675
Versione della politica 1675
Documento di policy JSON 1675
Ulteriori informazioni 1676

AutoScalingReadOnlyAccess 1676
Utilizzo di questa politica 1676
Dettagli della policy 1676
Versione della politica 1677
Documento di policy JSON 1677
Ulteriori informazioni 1677
AutoScalingServiceRolePolicy 1677
Utilizzo di questa politica 1677
Dettagli della policy 1678
Versione della politica 1678
Documento di policy JSON 1678
Ulteriori informazioni 1681
AWS-SSM-Automation-DiagnosisBucketPolicy 1681
Utilizzo di questa politica 1681
Dettagli della policy 1681
Versione della politica 1682
Documento di policy JSON 1682
Ulteriori informazioni 1684
AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy 1684
Utilizzo di questa politica 1685
Dettagli della policy 1685
Versione della politica 1685
Documento di policy JSON 1685
Ulteriori informazioni 1688
AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy 1688
Utilizzo di questa politica 1688
Dettagli della policy 1688
Versione della politica 1688
Documento di policy JSON 1689
Ulteriori informazioni 1691
AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy 1691
Utilizzo di questa politica 1691
Dettagli della policy 1691
Versione della politica 1691
Documento di policy JSON 1692
Ulteriori informazioni 1692

AWS-SSM-RemediationAutomation-AdministrationRolePolicy 1693
Utilizzo di questa politica 1693
Dettagli della policy 1693
Versione della politica 1693
Documento di policy JSON 1693
Ulteriori informazioni 1696
AWS-SSM-RemediationAutomation-ExecutionRolePolicy 1696
Utilizzo di questa politica 1696
Dettagli della policy 1696
Versione della politica 1697
Documento di policy JSON 1697
Ulteriori informazioni 1703
AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy 1703
Utilizzo di questa politica 1703
Dettagli della policy 1704
Versione della politica 1704
Documento di policy JSON 1704
Ulteriori informazioni 1705
AWS_ConfigRole 1705
Utilizzo di questa politica 1705
Dettagli della policy 1705
Versione della politica 1705
Documento sulla politica JSON 1706
Ulteriori informazioni 1760
AWSAccountActivityAccess 1760
Utilizzo di questa politica 1760
Dettagli della policy 1760
Versione della politica 1760
Documento di policy JSON 1760
Ulteriori informazioni 1761
AWSAccountManagementFullAccess 1761
Utilizzo di questa politica 1762
Dettagli della policy 1762
Versione della politica 1762
Documento di policy JSON 1762
Ulteriori informazioni 1762

AWSAccountManagementReadOnlyAccess 1763
Utilizzo di questa politica 1763
Dettagli della policy 1763
Versione della politica 1763
Documento di policy JSON 1763
Ulteriori informazioni 1764
AWSAccountSettingsManagementRole 1764
Utilizzo di questa politica 1764
Dettagli della policy 1764
Versione della politica 1764
Documento di policy JSON 1765
Ulteriori informazioni 1767
AWSAccountUsageReportAccess 1767
Utilizzo di questa politica 1768
Dettagli della policy 1768
Versione della politica 1768
Documento di policy JSON 1768
Ulteriori informazioni 1768
AWSAgentlessDiscoveryService 1769
Utilizzo di questa politica 1769
Dettagli della policy 1769
Versione della politica 1769
Documento di policy JSON 1769
Ulteriori informazioni 1771
AWSAppConfigServiceRolePolicy 1771
Utilizzo di questa politica 1771
Dettagli della policy 1772
Versione della politica 1772
Documento di policy JSON 1772
Ulteriori informazioni 1773
AWSAppFabricFullAccess 1773
Utilizzo di questa politica 1773
Dettagli della policy 1773
Versione della politica 1773
Documento di policy JSON 1773
Ulteriori informazioni 1775

AWSAppFabricReadOnlyAccess 1775
Utilizzo di questa politica 1775
Dettagli della policy 1775
Versione della politica 1775
Documento di policy JSON 1776
Ulteriori informazioni 1776
AWSAppFabricServiceRolePolicy 1776
Utilizzo di questa politica 1776
Dettagli della policy 1777
Versione della politica 1777
Documento di policy JSON 1777
Ulteriori informazioni 1778
AWSApplicationAutoscalingAppStreamFleetPolicy 1778
Utilizzo di questa politica 1778
Dettagli della policy 1779
Versione della politica 1779
Documento di policy JSON 1779
Ulteriori informazioni 1780
AWSApplicationAutoscalingCassandraTablePolicy 1780
Utilizzo di questa politica 1780
Dettagli della policy 1780
Versione della politica 1780
Documento di policy JSON 1780
Ulteriori informazioni 1781
AWSApplicationAutoscalingComprehendEndpointPolicy 1781
Utilizzo di questa politica 1781
Dettagli della policy 1782
Versione della politica 1782
Documento di policy JSON 1782
Ulteriori informazioni 1783
AWSApplicationAutoScalingCustomResourcePolicy 1783
Utilizzo di questa politica 1783
Dettagli della policy 1783
Versione della politica 1783
Documento di policy JSON 1783
Ulteriori informazioni 1784

AWSApplicationAutoscalingDynamoDBTablePolicy 1784
Utilizzo di questa politica 1784
Dettagli della policy 1784
Versione della politica 1785
Documento di policy JSON 1785
Ulteriori informazioni 1785
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 1785
Utilizzo di questa politica 1786
Dettagli della policy 1786
Versione della politica 1786
Documento di policy JSON 1786
Ulteriori informazioni 1787
AWSApplicationAutoscalingECSServicePolicy 1787
Utilizzo di questa politica 1787
Dettagli della policy 1787
Versione della politica 1787
Documento di policy JSON 1788
Ulteriori informazioni 1788
AWSApplicationAutoscalingElastiCacheRGPolicy 1788
Utilizzo di questa politica 1788
Dettagli della policy 1789
Versione della politica 1789
Documento di policy JSON 1789
Ulteriori informazioni 1790
AWSApplicationAutoscalingEMRInstanceGroupPolicy 1790
Utilizzo di questa politica 1790
Dettagli della policy 1790
Versione della politica 1791
Documento di policy JSON 1791
Ulteriori informazioni 1791
AWSApplicationAutoscalingKafkaClusterPolicy 1792
Utilizzo di questa politica 1792
Dettagli della policy 1792
Versione della politica 1792
Documento di policy JSON 1792
Ulteriori informazioni 1793

AWSApplicationAutoscalingLambdaConcurrencyPolicy 1793
Utilizzo di questa politica 1793
Dettagli della policy 1793
Versione della politica 1793
Documento di policy JSON 1794
Ulteriori informazioni 1794
AWSApplicationAutoscalingNeptuneClusterPolicy 1794
Utilizzo di questa politica 1795
Dettagli della policy 1795
Versione della politica 1795
Documento di policy JSON 1795
Ulteriori informazioni 1797
AWSApplicationAutoscalingRDSClusterPolicy 1797
Utilizzo di questa politica 1797
Dettagli della policy 1797
Versione della politica 1797
Documento di policy JSON 1797
Ulteriori informazioni 1798
AWSApplicationAutoscalingSageMakerEndpointPolicy 1798
Utilizzo di questa politica 1799
Dettagli della policy 1799
Versione della politica 1799
Documento di policy JSON 1799
Ulteriori informazioni 1800
AWSApplicationAutoscalingWorkSpacesPoolPolicy 1800
Utilizzo di questa politica 1800
Dettagli della policy 1800
Versione della politica 1801
Documento di policy JSON 1801
Ulteriori informazioni 1802
AWSApplicationDiscoveryAgentAccess 1802
Utilizzo di questa politica 1802
Dettagli della policy 1803
Versione della politica 1803
Documento di policy JSON 1803
Ulteriori informazioni 1803

AWSApplicationDiscoveryAgentlessCollectorAccess 1804
Utilizzo di questa politica 1804
Dettagli della policy 1804
Versione della politica 1804
Documento di policy JSON 1804
Ulteriori informazioni 1805
AWSApplicationDiscoveryServiceFullAccess 1806
Utilizzo di questa politica 1806
Dettagli della policy 1806
Versione della politica 1806
Documento di policy JSON 1806
Ulteriori informazioni 1808
AWSApplicationMigrationAgentInstallationPolicy 1808
Utilizzo di questa politica 1808
Dettagli della policy 1808
Versione della politica 1809
Documento di policy JSON 1809
Ulteriori informazioni 1810
AWSApplicationMigrationAgentPolicy 1810
Utilizzo di questa politica 1810
Dettagli della policy 1810
Versione della politica 1810
Documento di policy JSON 1811
Ulteriori informazioni 1811
AWSApplicationMigrationAgentPolicy_v2 1812
Utilizzo di questa politica 1812
Dettagli della policy 1812
Versione della politica 1812
Documento di policy JSON 1812
Ulteriori informazioni 1813
AWSApplicationMigrationConversionServerPolicy 1813
Utilizzo di questa politica 1814
Dettagli della policy 1814
Versione della politica 1814
Documento di policy JSON 1814
Ulteriori informazioni 1815

AWSApplicationMigrationEC2Access 1815
Utilizzo di questa politica 1815
Dettagli della policy 1815
Versione della politica 1815
Documento di policy JSON 1815
Ulteriori informazioni 1824
AWSApplicationMigrationFSxProxyPolicy 1824
Utilizzo di questa politica 1824
Dettagli della policy 1824
Versione della politica 1824
Documento di policy JSON 1824
Ulteriori informazioni 1826
AWSApplicationMigrationFSxProxyVPCPolicy 1826
Utilizzo di questa politica 1827
Dettagli della policy 1827
Versione della politica 1827
Documento di policy JSON 1827
Ulteriori informazioni 1831
AWSApplicationMigrationFullAccess 1832
Utilizzo di questa politica 1832
Dettagli della policy 1832
Versione della politica 1832
Documento sulla politica JSON 1832
Ulteriori informazioni 1841
AWSApplicationMigrationMGHAccess 1841
Utilizzo di questa politica 1841
Dettagli della policy 1841
Versione della politica 1841
Documento di policy JSON 1842
Ulteriori informazioni 1842
AWSApplicationMigrationNetworkMigrationCustomResource 1842
Utilizzo di questa politica 1842
Dettagli della policy 1843
Versione della politica 1843
Documento di policy JSON 1843
Ulteriori informazioni 1844

AWSApplicationMigrationNetworkMigrationMultiAccount 1844
Utilizzo di questa politica 1844
Dettagli della policy 1844
Versione della politica 1844
Documento sulla politica JSON 1845
Ulteriori informazioni 1870
AWSApplicationMigrationReadOnlyAccess 1870
Utilizzo di questa politica 1870
Dettagli della policy 1870
Versione della politica 1870
Documento di policy JSON 1871
Ulteriori informazioni 1872
AWSApplicationMigrationReplicationServerPolicy 1872
Utilizzo di questa politica 1872
Dettagli della policy 1872
Versione della politica 1873
Documento di policy JSON 1873
Ulteriori informazioni 1875
AWSApplicationMigrationServiceEc2InstancePolicy 1875
Utilizzo di questa politica 1875
Dettagli della policy 1875
Versione della politica 1875
Documento di policy JSON 1876
Ulteriori informazioni 1877
AWSApplicationMigrationServiceRolePolicy 1877
Utilizzo di questa politica 1877
Dettagli della policy 1877
Versione della politica 1877
Documento sulla politica JSON 1878
Ulteriori informazioni 1885
AWSApplicationMigrationSSMAccess 1885
Utilizzo di questa politica 1885
Dettagli della policy 1885
Versione della politica 1886
Documento di policy JSON 1886
Ulteriori informazioni 1888

AWSApplicationMigrationVCenterClientPolicy 1888
Utilizzo di questa politica 1888
Dettagli della policy 1888
Versione della politica 1888
Documento di policy JSON 1889
Ulteriori informazioni 1889
AWSAppMeshEnvoyAccess 1889
Utilizzo di questa politica 1890
Dettagli della policy 1890
Versione della politica 1890
Documento di policy JSON 1890
Ulteriori informazioni 1890
AWSAppMeshFullAccess 1891
Utilizzo di questa politica 1891
Dettagli della policy 1891
Versione della politica 1891
Documento di policy JSON 1891
Ulteriori informazioni 1893
AWSAppMeshPreviewEnvoyAccess 1893
Utilizzo di questa politica 1893
Dettagli della policy 1893
Versione della politica 1893
Documento di policy JSON 1894
Ulteriori informazioni 1894
AWSAppMeshPreviewServiceRolePolicy 1894
Utilizzo di questa politica 1894
Dettagli della policy 1894
Versione della politica 1895
Documento di policy JSON 1895
Ulteriori informazioni 1895
AWSAppMeshReadOnly 1896
Utilizzo di questa politica 1896
Dettagli della policy 1896
Versione della politica 1896
Documento di policy JSON 1896
Ulteriori informazioni 1897

AWSAppMeshServiceRolePolicy 1897
Utilizzo di questa politica 1898
Dettagli della policy 1898
Versione della politica 1898
Documento di policy JSON 1898
Ulteriori informazioni 1899
AWSAppRunnerFullAccess 1899
Utilizzo di questa politica 1899
Dettagli della policy 1899
Versione della politica 1899
Documento di policy JSON 1899
Ulteriori informazioni 1900
AWSAppRunnerReadOnlyAccess 1901
Utilizzo di questa politica 1901
Dettagli della policy 1901
Versione della politica 1901
Documento di policy JSON 1901
Ulteriori informazioni 1902
AWSAppRunnerServicePolicyForECRAccess 1902
Utilizzo di questa politica 1902
Dettagli della policy 1902
Versione della politica 1902
Documento di policy JSON 1903
Ulteriori informazioni 1903
AWSAppSyncAdministrator 1903
Utilizzo di questa politica 1903
Dettagli della policy 1904
Versione della politica 1904
Documento di policy JSON 1904
Ulteriori informazioni 1905
AWSAppSyncInvokeFullAccess 1905
Utilizzo di questa politica 1905
Dettagli della policy 1906
Versione della politica 1906
Documento di policy JSON 1906
Ulteriori informazioni 1906

AWSAppSyncPushToCloudWatchLogs 1907
Utilizzo di questa politica 1907
Dettagli della policy 1907
Versione della politica 1907
Documento di policy JSON 1907
Ulteriori informazioni 1908
AWSAppSyncSchemaAuthor 1908
Utilizzo di questa politica 1908
Dettagli della policy 1908
Versione della politica 1908
Documento di policy JSON 1909
Ulteriori informazioni 1910
AWSAppSyncServiceRolePolicy 1910
Utilizzo di questa politica 1910
Dettagli della policy 1910
Versione della politica 1910
Documento di policy JSON 1910
Ulteriori informazioni 1911
AWSArtifactAccountSync 1911
Utilizzo di questa politica 1911
Dettagli della policy 1911
Versione della politica 1912
Documento di policy JSON 1912
Ulteriori informazioni 1912
AWSArtifactAgreementsFullAccess 1912
Utilizzo di questa politica 1913
Dettagli della policy 1913
Versione della politica 1913
Documento di policy JSON 1913
Ulteriori informazioni 1915
AWSArtifactAgreementsReadOnlyAccess 1915
Utilizzo di questa politica 1916
Dettagli della policy 1916
Versione della politica 1916
Documento di policy JSON 1916
Ulteriori informazioni 1917

AWSArtifactComplianceInquiriesFullAccess 1917
Utilizzo di questa politica 1917
Dettagli della policy 1918
Versione della politica 1918
Documento sulla politica JSON 1918
Ulteriori informazioni 1919
AWSArtifactComplianceInquiriesReadOnlyAccess 1919
Utilizzo di questa politica 1919
Dettagli della policy 1919
Versione della politica 1919
Documento di policy JSON 1920
Ulteriori informazioni 1920
AWSArtifactReportsReadOnlyAccess 1920
Utilizzo di questa politica 1921
Dettagli della policy 1921
Versione della politica 1921
Documento di policy JSON 1921
Ulteriori informazioni 1922
AWSArtifactServiceRolePolicy 1922
Utilizzo di questa politica 1922
Dettagli della policy 1922
Versione della politica 1922
Documento di policy JSON 1923
Ulteriori informazioni 1923
AWSAuditManagerAdministratorAccess 1923
Utilizzo di questa politica 1923
Dettagli della policy 1923
Versione della politica 1924
Documento di policy JSON 1924
Ulteriori informazioni 1928
AWSAuditManagerServiceRolePolicy 1928
Utilizzo di questa politica 1928
Dettagli della policy 1928
Versione della politica 1928
Documento di policy JSON 1929
Ulteriori informazioni 1935

AWSAutoScalingPlansEC2AutoScalingPolicy 1936
Utilizzo di questa politica 1936
Dettagli della policy 1936
Versione della politica 1936
Documento di policy JSON 1936
Ulteriori informazioni 1937
AWSBackupAuditAccess 1937
Utilizzo di questa politica 1937
Dettagli della policy 1937
Versione della politica 1938
Documento di policy JSON 1938
Ulteriori informazioni 1939
AWSBackupDataTransferAccess 1939
Utilizzo di questa politica 1939
Dettagli della policy 1939
Versione della politica 1940
Documento di policy JSON 1940
Ulteriori informazioni 1940
AWSBackupFullAccess 1941
Utilizzo di questa politica 1941
Dettagli della policy 1941
Versione della politica 1941
Documento di policy JSON 1941
Ulteriori informazioni 1953
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 1953
Utilizzo di questa politica 1953
Dettagli della policy 1953
Versione della politica 1954
Documento di policy JSON 1954
Ulteriori informazioni 1955
AWSBackupGuardDutyRolePolicyForScans 1955
Utilizzo di questa politica 1955
Dettagli della policy 1955
Versione della politica 1955
Documento di policy JSON 1955
Ulteriori informazioni 1959

AWSBackupOperatorAccess 1960
Utilizzo di questa politica 1960
Dettagli della policy 1960
Versione della politica 1960
Documento di policy JSON 1960
Ulteriori informazioni 1969
AWSBackupOrganizationAdminAccess 1970
Utilizzo di questa politica 1970
Dettagli della policy 1970
Versione della politica 1970
Documento di policy JSON 1970
Ulteriori informazioni 1972
AWSBackupRestoreAccessForSAPHANA 1972
Utilizzo di questa politica 1972
Dettagli della policy 1973
Versione della politica 1973
Documento di policy JSON 1973
Ulteriori informazioni 1974
AWSBackupSearchOperatorAccess 1974
Utilizzo di questa politica 1974
Dettagli della policy 1974
Versione della politica 1975
Documento di policy JSON 1975
Ulteriori informazioni 1976
AWSBackupServiceLinkedRolePolicyForBackup 1977
Utilizzo di questa politica 1977
Dettagli della policy 1977
Versione della politica 1977
Documento di policy JSON 1977
Ulteriori informazioni 1987
AWSBackupServiceLinkedRolePolicyForBackupTest 1988
Utilizzo di questa politica 1988
Dettagli della policy 1988
Versione della politica 1988
Documento di policy JSON 1988
Ulteriori informazioni 1989

AWSBackupServiceRolePolicyForBackup 1989
Utilizzo di questa politica 1989
Dettagli della policy 1989
Versione della politica 1990
Documento di policy JSON 1990
Ulteriori informazioni 2004
AWSBackupServiceRolePolicyForIndexing 2005
Utilizzo di questa politica 2005
Dettagli della policy 2005
Versione della politica 2005
Documento di policy JSON 2005
Ulteriori informazioni 2006
AWSBackupServiceRolePolicyForItemRestores 2007
Utilizzo di questa politica 2007
Dettagli della policy 2007
Versione della politica 2007
Documento di policy JSON 2007
Ulteriori informazioni 2009
AWSBackupServiceRolePolicyForRestores 2009
Utilizzo di questa politica 2009
Dettagli della policy 2010
Versione della politica 2010
Documento di policy JSON 2010
Ulteriori informazioni 2024
AWSBackupServiceRolePolicyForS3Backup 2024
Utilizzo di questa politica 2024
Dettagli della policy 2024
Versione della politica 2025
Documento di policy JSON 2025
Ulteriori informazioni 2027
AWSBackupServiceRolePolicyForS3Restore 2027
Utilizzo di questa politica 2027
Dettagli della policy 2028
Versione della politica 2028
Documento di policy JSON 2028
Ulteriori informazioni 2029

AWSBackupServiceRolePolicyForScans 2030
Utilizzo di questa politica 2030
Dettagli della policy 2030
Versione della politica 2030
Documento di policy JSON 2030
Ulteriori informazioni 2031
AWSBatchFullAccess 2031
Utilizzo di questa politica 2031
Dettagli della policy 2032
Versione della politica 2032
Documento di policy JSON 2032
Ulteriori informazioni 2033
AWSBatchServiceEventTargetRole 2034
Utilizzo di questa politica 2034
Dettagli della policy 2034
Versione della politica 2034
Documento di policy JSON 2034
Ulteriori informazioni 2035
AWSBatchServiceRole 2035
Utilizzo di questa politica 2035
Dettagli della policy 2035
Versione della politica 2035
Documento di policy JSON 2035
Ulteriori informazioni 2039
AWSBatchServiceRolePolicyForSageMaker 2039
Utilizzo di questa politica 2039
Dettagli della policy 2039
Versione della politica 2039
Documento di policy JSON 2040
Ulteriori informazioni 2041
AWSBCMDataExportsServiceRolePolicy 2041
Utilizzo di questa politica 2041
Dettagli della policy 2041
Versione della politica 2042
Documento di policy JSON 2042
Ulteriori informazioni 2042

AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy 2042
Utilizzo di questa politica 2043
Dettagli della policy 2043
Versione della politica 2043
Documento di policy JSON 2043
Ulteriori informazioni 2045
AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy 2045
Utilizzo di questa politica 2045
Dettagli della policy 2045
Versione della politica 2045
Documento di policy JSON 2046
Ulteriori informazioni 2047
AWSBillingConductorFullAccess 2047
Utilizzo di questa politica 2048
Dettagli della policy 2048
Versione della politica 2048
Documento di policy JSON 2048
Ulteriori informazioni 2049
AWSBillingConductorReadOnlyAccess 2049
Utilizzo di questa politica 2049
Dettagli della policy 2049
Versione della politica 2049
Documento di policy JSON 2050
Ulteriori informazioni 2050
AWSBillingReadOnlyAccess 2050
Utilizzo di questa politica 2051
Dettagli della policy 2051
Versione della politica 2051
Documento sulla politica JSON 2051
Ulteriori informazioni 2053
AWSBillingServiceRolePolicy 2053
Utilizzo di questa politica 2054
Dettagli della policy 2054
Versione della politica 2054
Documento di policy JSON 2054
Ulteriori informazioni 2054

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 2055
Utilizzo di questa politica 2055
Dettagli della policy 2055
Versione della politica 2055
Documento di policy JSON 2055
Ulteriori informazioni 2056
AWSBudgetsActionsWithAWSResourceControlAccess 2057
Utilizzo di questa politica 2057
Dettagli della policy 2057
Versione della politica 2057
Documento di policy JSON 2057
Ulteriori informazioni 2059
AWSBudgetsReadOnlyAccess 2059
Utilizzo di questa politica 2059
Dettagli della policy 2059
Versione della politica 2059
Documento di policy JSON 2059
Ulteriori informazioni 2060
AWSBudgetsSpendLimitMemberRolePolicy 2060
Utilizzo di questa politica 2060
Dettagli della policy 2060
Versione della politica 2061
Documento sulla politica JSON 2061
Ulteriori informazioni 2065
AWSBugBustFullAccess 2065
Utilizzo di questa politica 2065
Dettagli della policy 2065
Versione della politica 2066
Documento di policy JSON 2066
Ulteriori informazioni 2067
AWSBugBustPlayerAccess 2067
Utilizzo di questa politica 2067
Dettagli della policy 2067
Versione della politica 2068
Documento di policy JSON 2068
Ulteriori informazioni 2069

AWSBugBustServiceRolePolicy 2069
Utilizzo di questa politica 2069
Dettagli della policy 2069
Versione della politica 2069
Documento di policy JSON 2070
Ulteriori informazioni 2070
AWSCertificateManagerFullAccess 2070
Utilizzo di questa politica 2070
Dettagli della policy 2071
Versione della politica 2071
Documento di policy JSON 2071
Ulteriori informazioni 2072
AWSCertificateManagerPrivateCAAuditor 2072
Utilizzo di questa politica 2072
Dettagli della policy 2072
Versione della politica 2073
Documento di policy JSON 2073
Ulteriori informazioni 2073
AWSCertificateManagerPrivateCAFullAccess 2074
Utilizzo di questa politica 2074
Dettagli della policy 2074
Versione della politica 2074
Documento di policy JSON 2074
Ulteriori informazioni 2075
AWSCertificateManagerPrivateCAPrivilegedUser 2075
Utilizzo di questa politica 2075
Dettagli della policy 2075
Versione della politica 2075
Documento di policy JSON 2076
Ulteriori informazioni 2077
AWSCertificateManagerPrivateCAReadOnly 2077
Utilizzo di questa politica 2077
Dettagli della policy 2077
Versione della politica 2078
Documento di policy JSON 2078
Ulteriori informazioni 2078

AWSCertificateManagerPrivateCAUser 2079
Utilizzo di questa politica 2079
Dettagli della policy 2079
Versione della politica 2079
Documento di policy JSON 2079
Ulteriori informazioni 2080
AWSCertificateManagerReadOnly 2081
Utilizzo di questa politica 2081
Dettagli della policy 2081
Versione della politica 2081
Documento di policy JSON 2081
Ulteriori informazioni 2082
AWSChatbotServiceLinkedRolePolicy 2082
Utilizzo di questa politica 2082
Dettagli della policy 2082
Versione della politica 2083
Documento di policy JSON 2083
Ulteriori informazioni 2084
AWSCleanRoomsFullAccess 2084
Utilizzo di questa politica 2084
Dettagli della policy 2084
Versione della politica 2084
Documento di policy JSON 2084
Ulteriori informazioni 2089
AWSCleanRoomsFullAccessNoQuerying 2089
Utilizzo di questa politica 2089
Dettagli della policy 2089
Versione della politica 2089
Documento di policy JSON 2090
Ulteriori informazioni 2094
AWSCleanRoomsMLFullAccess 2095
Utilizzo di questa politica 2095
Dettagli della policy 2095
Versione della politica 2095
Documento di policy JSON 2095
Ulteriori informazioni 2099

AWSCleanRoomsMLReadOnlyAccess 2099
Utilizzo di questa politica 2100
Dettagli della policy 2100
Versione della politica 2100
Documento di policy JSON 2100
Ulteriori informazioni 2101
AWSCleanRoomsReadOnlyAccess 2101
Utilizzo di questa politica 2102
Dettagli della policy 2102
Versione della politica 2102
Documento di policy JSON 2102
Ulteriori informazioni 2103
AWSCleanRoomsServiceRolePolicy 2104
Utilizzo di questa politica 2104
Dettagli della policy 2104
Versione della politica 2104
Documento di policy JSON 2104
Ulteriori informazioni 2105
AWSCloud9Administrator 2105
Utilizzo di questa politica 2105
Dettagli della policy 2105
Versione della politica 2105
Documento di policy JSON 2106
Ulteriori informazioni 2107
AWSCloud9EnvironmentMember 2107
Utilizzo di questa politica 2108
Dettagli della policy 2108
Versione della politica 2108
Documento di policy JSON 2108
Ulteriori informazioni 2110
AWSCloud9ServiceRolePolicy 2110
Utilizzo di questa politica 2110
Dettagli della policy 2110
Versione della politica 2110
Documento di policy JSON 2111
Ulteriori informazioni 2113

AWSCloud9SSMInstanceProfile 2113
Utilizzo di questa politica 2113
Dettagli della policy 2113
Versione della politica 2114
Documento di policy JSON 2114
Ulteriori informazioni 2114
AWSCloud9User 2114
Utilizzo di questa politica 2115
Dettagli della policy 2115
Versione della politica 2115
Documento di policy JSON 2115
Ulteriori informazioni 2118
AWSCloudFormationFullAccess 2118
Utilizzo di questa politica 2118
Dettagli della policy 2118
Versione della politica 2118
Documento di policy JSON 2118
Ulteriori informazioni 2119
AWSCloudFormationReadOnlyAccess 2119
Utilizzo di questa politica 2119
Dettagli della policy 2119
Versione della politica 2120
Documento di policy JSON 2120
Ulteriori informazioni 2120
AWSCloudFrontLogger 2120
Utilizzo di questa politica 2121
Dettagli della policy 2121
Versione della politica 2121
Documento di policy JSON 2121
Ulteriori informazioni 2122
AWSCloudFrontVPCOriginServiceRolePolicy 2122
Utilizzo di questa politica 2122
Dettagli della policy 2122
Versione della politica 2122
Documento di policy JSON 2122
Ulteriori informazioni 2125

AWSCloudHSMFullAccess 2125
Utilizzo di questa politica 2125
Dettagli della policy 2125
Versione della politica 2126
Documento di policy JSON 2126
Ulteriori informazioni 2126
AWSCloudHSMReadOnlyAccess 2126
Utilizzo di questa politica 2127
Dettagli della policy 2127
Versione della politica 2127
Documento di policy JSON 2127
Ulteriori informazioni 2127
AWSCloudHSMRole 2128
Utilizzo di questa politica 2128
Dettagli della policy 2128
Versione della politica 2128
Documento di policy JSON 2128
Ulteriori informazioni 2129
AWSCloudMapDiscoverInstanceAccess 2129
Utilizzo di questa politica 2129
Dettagli della policy 2129
Versione della politica 2130
Documento di policy JSON 2130
Ulteriori informazioni 2130
AWSCloudMapFullAccess 2130
Utilizzo di questa politica 2131
Dettagli della policy 2131
Versione della politica 2131
Documento di policy JSON 2131
Ulteriori informazioni 2132
AWSCloudMapReadOnlyAccess 2132
Utilizzo di questa politica 2132
Dettagli della policy 2132
Versione della politica 2132
Documento di policy JSON 2133
Ulteriori informazioni 2133

AWSCloudMapRegisterInstanceAccess 2133
Utilizzo di questa politica 2133
Dettagli della policy 2134
Versione della politica 2134
Documento di policy JSON 2134
Ulteriori informazioni 2135
AWSCloudShellFullAccess 2135
Utilizzo di questa politica 2135
Dettagli della policy 2135
Versione della politica 2135
Documento di policy JSON 2136
Ulteriori informazioni 2136
AWSCloudTrail_FullAccess 2136
Utilizzo di questa politica 2136
Dettagli della policy 2136
Versione della politica 2137
Documento di policy JSON 2137
Ulteriori informazioni 2139
AWSCloudTrail_ReadOnlyAccess 2139
Utilizzo di questa politica 2140
Dettagli della policy 2140
Versione della politica 2140
Documento di policy JSON 2140
Ulteriori informazioni 2141
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 2141
Utilizzo di questa politica 2141
Dettagli della policy 2141
Versione della politica 2141
Documento di policy JSON 2142
Ulteriori informazioni 2142
AWSCodeArtifactAdminAccess 2142
Utilizzo di questa politica 2142
Dettagli della policy 2142
Versione della politica 2143
Documento di policy JSON 2143
Ulteriori informazioni 2143

AWSCodeArtifactReadOnlyAccess 2144
Utilizzo di questa politica 2144
Dettagli della policy 2144
Versione della politica 2144
Documento di policy JSON 2144
Ulteriori informazioni 2145
AWSCodeBuildAdminAccess 2145
Utilizzo di questa politica 2145
Dettagli della policy 2145
Versione della politica 2146
Documento di policy JSON 2146
Ulteriori informazioni 2149
AWSCodeBuildDeveloperAccess 2150
Utilizzo di questa politica 2150
Dettagli della policy 2150
Versione della politica 2150
Documento di policy JSON 2150
Ulteriori informazioni 2153
AWSCodeBuildReadOnlyAccess 2153
Utilizzo di questa politica 2153
Dettagli della policy 2154
Versione della politica 2154
Documento di policy JSON 2154
Ulteriori informazioni 2155
AWSCodeCommitFullAccess 2156
Utilizzo di questa politica 2156
Dettagli della policy 2156
Versione della politica 2156
Documento di policy JSON 2156
Ulteriori informazioni 2161
AWSCodeCommitPowerUser 2161
Utilizzo di questa politica 2161
Dettagli della policy 2161
Versione della politica 2162
Documento di policy JSON 2162
Ulteriori informazioni 2167

AWSCodeCommitReadOnly 2167
Utilizzo di questa politica 2167
Dettagli della policy 2167
Versione della politica 2167
Documento di policy JSON 2167
Ulteriori informazioni 2170
AWSCodeDeployDeployerAccess 2170
Utilizzo di questa politica 2170
Dettagli della policy 2170
Versione della politica 2171
Documento di policy JSON 2171
Ulteriori informazioni 2172
AWSCodeDeployFullAccess 2173
Utilizzo di questa politica 2173
Dettagli della policy 2173
Versione della politica 2173
Documento di policy JSON 2173
Ulteriori informazioni 2175
AWSCodeDeployReadOnlyAccess 2175
Utilizzo di questa politica 2175
Dettagli della policy 2175
Versione della politica 2175
Documento di policy JSON 2176
Ulteriori informazioni 2177
AWSCodeDeployRole 2177
Utilizzo di questa politica 2177
Dettagli della policy 2177
Versione della politica 2177
Documento di policy JSON 2178
Ulteriori informazioni 2179
AWSCodeDeployRoleForCloudFormation 2179
Utilizzo di questa politica 2179
Dettagli della policy 2179
Versione della politica 2180
Documento di policy JSON 2180
Ulteriori informazioni 2180

AWSCodeDeployRoleForECS 2180
Utilizzo di questa politica 2181
Dettagli della policy 2181
Versione della politica 2181
Documento di policy JSON 2181
Ulteriori informazioni 2182
AWSCodeDeployRoleForECSLimited 2182
Utilizzo di questa politica 2182
Dettagli della policy 2183
Versione della politica 2183
Documento di policy JSON 2183
Ulteriori informazioni 2185
AWSCodeDeployRoleForLambda 2185
Utilizzo di questa politica 2185
Dettagli della policy 2185
Versione della politica 2185
Documento di policy JSON 2186
Ulteriori informazioni 2187
AWSCodeDeployRoleForLambdaLimited 2187
Utilizzo di questa politica 2187
Dettagli della policy 2187
Versione della politica 2187
Documento di policy JSON 2188
Ulteriori informazioni 2189
AWSCodePipeline_FullAccess 2189
Utilizzo di questa politica 2189
Dettagli della policy 2189
Versione della politica 2189
Documento di policy JSON 2190
Ulteriori informazioni 2193
AWSCodePipeline_ReadOnlyAccess 2193
Utilizzo di questa politica 2194
Dettagli della policy 2194
Versione della politica 2194
Documento di policy JSON 2194
Ulteriori informazioni 2195

AWSCodePipelineApproverAccess 2195
Utilizzo di questa politica 2196
Dettagli della policy 2196
Versione della politica 2196
Documento di policy JSON 2196
Ulteriori informazioni 2197
AWSCodePipelineCustomActionAccess 2197
Utilizzo di questa politica 2197
Dettagli della policy 2197
Versione della politica 2197
Documento di policy JSON 2197
Ulteriori informazioni 2198
AWSCodeStarFullAccess 2198
Utilizzo di questa politica 2198
Dettagli della policy 2198
Versione della politica 2199
Documento di policy JSON 2199
Ulteriori informazioni 2200
AWSCodeStarNotificationsServiceRolePolicy 2200
Utilizzo di questa politica 2200
Dettagli della policy 2200
Versione della politica 2200
Documento di policy JSON 2201
Ulteriori informazioni 2202
AWSCodeStarServiceRole 2202
Utilizzo di questa politica 2202
Dettagli della policy 2202
Versione della politica 2202
Documento di policy JSON 2203
Ulteriori informazioni 2207
AWSCompromisedKeyQuarantine 2208
Utilizzo di questa politica 2208
Dettagli della policy 2208
Versione della politica 2208
Documento di policy JSON 2208
Ulteriori informazioni 2209

AWSCompromisedKeyQuarantineV2 2210
Utilizzo di questa politica 2210
Dettagli della policy 2210
Versione della politica 2210
Documento di policy JSON 2210
Ulteriori informazioni 2213
AWSCompromisedKeyQuarantineV3 2213
Utilizzo di questa politica 2213
Dettagli della policy 2213
Versione della politica 2213
Documento di policy JSON 2214
Ulteriori informazioni 2217
AWSConfigMultiAccountSetupPolicy 2217
Utilizzo di questa politica 2217
Dettagli della policy 2217
Versione della politica 2217
Documento di policy JSON 2218
Ulteriori informazioni 2219
AWSConfigRemediationServiceRolePolicy 2220
Utilizzo di questa politica 2220
Dettagli della policy 2220
Versione della politica 2220
Documento di policy JSON 2220
Ulteriori informazioni 2221
AWSConfigRoleForOrganizations 2221
Utilizzo di questa politica 2221
Dettagli della policy 2221
Versione della politica 2222
Documento di policy JSON 2222
Ulteriori informazioni 2222
AWSConfigRulesExecutionRole 2222
Utilizzo di questa politica 2223
Dettagli della policy 2223
Versione della politica 2223
Documento di policy JSON 2223
Ulteriori informazioni 2224

AWSConfigServiceRolePolicy 2224
Utilizzo di questa politica 2224
Dettagli della policy 2224
Versione della politica 2224
Documento sulla politica JSON 2225
Ulteriori informazioni 2280
AWSConfigThirdPartyServiceRolePolicy 2280
Utilizzo di questa politica 2280
Dettagli della policy 2280
Versione della politica 2280
Documento di policy JSON 2280
Ulteriori informazioni 2281
AWSConfigUserAccess 2282
Utilizzo di questa politica 2282
Dettagli della policy 2282
Versione della politica 2282
Documento di policy JSON 2282
Ulteriori informazioni 2283
AWSConnector 2283
Utilizzo di questa politica 2283
Dettagli della policy 2283
Versione della politica 2284
Documento sulla politica JSON 2284
Ulteriori informazioni 2286
AWSControlTowerAccountServiceRolePolicy 2286
Utilizzo di questa politica 2286
Dettagli della policy 2286
Versione della politica 2286
Documento di policy JSON 2287
Ulteriori informazioni 2292
AWSControlTowerCloudTrailRolePolicy 2292
Utilizzo di questa politica 2292
Dettagli della policy 2292
Versione della politica 2292
Documento di policy JSON 2293
Ulteriori informazioni 2293

AWSControlTowerIdentityCenterManagementPolicy 2293
Utilizzo di questa politica 2294
Dettagli della policy 2294
Versione della politica 2294
Documento di policy JSON 2294
Ulteriori informazioni 2295
AWSControlTowerServiceRolePolicy 2295
Utilizzo di questa politica 2296
Dettagli della policy 2296
Versione della politica 2296
Documento di policy JSON 2296
Ulteriori informazioni 2301
AWSCostAndUsageReportAutomationPolicy 2301
Utilizzo di questa politica 2302
Dettagli della policy 2302
Versione della politica 2302
Documento di policy JSON 2302
Ulteriori informazioni 2303
AWSDataExchangeDataGrantOwnerFullAccess 2303
Utilizzo di questa politica 2303
Dettagli della policy 2304
Versione della politica 2304
Documento di policy JSON 2304
Ulteriori informazioni 2305
AWSDataExchangeDataGrantReceiverFullAccess 2306
Utilizzo di questa politica 2306
Dettagli della policy 2306
Versione della politica 2306
Documento di policy JSON 2306
Ulteriori informazioni 2308
AWSDataExchangeFullAccess 2308
Utilizzo di questa politica 2308
Dettagli della policy 2308
Versione della politica 2309
Documento di policy JSON 2309
Ulteriori informazioni 2312

AWSDataExchangeProviderFullAccess 2312
Utilizzo di questa politica 2313
Dettagli della policy 2313
Versione della politica 2313
Documento di policy JSON 2313
Ulteriori informazioni 2317
AWSDataExchangeReadOnly 2317
Utilizzo di questa politica 2317
Dettagli della policy 2317
Versione della politica 2318
Documento di policy JSON 2318
Ulteriori informazioni 2319
AWSDataExchangeServiceRolePolicyForLicenseManagement 2319
Utilizzo di questa politica 2319
Dettagli della policy 2319
Versione della politica 2320
Documento di policy JSON 2320
Ulteriori informazioni 2320
AWSDataExchangeServiceRolePolicyForOrganizationDiscovery 2321
Utilizzo di questa politica 2321
Dettagli della policy 2321
Versione della politica 2321
Documento di policy JSON 2321
Ulteriori informazioni 2322
AWSDataExchangeSubscriberFullAccess 2322
Utilizzo di questa politica 2322
Dettagli della policy 2322
Versione della politica 2322
Documento di policy JSON 2323
Ulteriori informazioni 2325
AWSDataLifecycleManagerServiceRole 2325
Utilizzo di questa politica 2325
Dettagli della policy 2325
Versione della politica 2326
Documento di policy JSON 2326
Ulteriori informazioni 2327

AWSDataLifecycleManagerServiceRoleForAMIManagement 2327
Utilizzo di questa politica 2327
Dettagli della policy 2327
Versione della politica 2328
Documento di policy JSON 2328
Ulteriori informazioni 2329
AWSDataLifecycleManagerSSMFullAccess 2329
Utilizzo di questa politica 2329
Dettagli della policy 2330
Versione della politica 2330
Documento di policy JSON 2330
Ulteriori informazioni 2331
AWSDataPipeline_FullAccess 2332
Utilizzo di questa politica 2332
Dettagli della policy 2332
Versione della politica 2332
Documento di policy JSON 2332
Ulteriori informazioni 2333
AWSDataPipeline_PowerUser 2333
Utilizzo di questa politica 2333
Dettagli della policy 2334
Versione della politica 2334
Documento di policy JSON 2334
Ulteriori informazioni 2335
AWSDataSyncDiscoveryServiceRolePolicy 2335
Utilizzo di questa politica 2335
Dettagli della policy 2335
Versione della politica 2336
Documento di policy JSON 2336
Ulteriori informazioni 2337
AWSDataSyncFullAccess 2337
Utilizzo di questa politica 2337
Dettagli della policy 2337
Versione della politica 2337
Documento di policy JSON 2338
Ulteriori informazioni 2340

AWSDataSyncReadOnlyAccess 2340
Utilizzo di questa politica 2340
Dettagli della policy 2340
Versione della politica 2341
Documento di policy JSON 2341
Ulteriori informazioni 2341
AWSDataSyncServiceRolePolicy 2342
Utilizzo di questa politica 2342
Dettagli della policy 2342
Versione della politica 2342
Documento di policy JSON 2342
Ulteriori informazioni 2343
AWSDeadlineCloud-FleetWorker 2344
Utilizzo di questa politica 2344
Dettagli della policy 2344
Versione della politica 2344
Documento di policy JSON 2344
Ulteriori informazioni 2345
AWSDeadlineCloud-UserAccessFarms 2345
Utilizzo di questa politica 2345
Dettagli della policy 2345
Versione della politica 2346
Documento di policy JSON 2346
Ulteriori informazioni 2352
AWSDeadlineCloud-UserAccessFleets 2352
Utilizzo di questa politica 2352
Dettagli della policy 2352
Versione della politica 2353
Documento di policy JSON 2353
Ulteriori informazioni 2356
AWSDeadlineCloud-UserAccessJobs 2357
Utilizzo di questa politica 2357
Dettagli della policy 2357
Versione della politica 2357
Documento di policy JSON 2357
Ulteriori informazioni 2361

AWSDeadlineCloud-UserAccessQueues 2361
Utilizzo di questa politica 2362
Dettagli della policy 2362
Versione della politica 2362
Documento di policy JSON 2362
Ulteriori informazioni 2367
AWSDeadlineCloud-WorkerHost 2367
Utilizzo di questa politica 2367
Dettagli della policy 2367
Versione della politica 2367
Documento di policy JSON 2368
Ulteriori informazioni 2369
AWSDeepLensLambdaFunctionAccessPolicy 2369
Utilizzo di questa politica 2369
Dettagli della policy 2369
Versione della politica 2370
Documento di policy JSON 2370
Ulteriori informazioni 2371
AWSDeepLensServiceRolePolicy 2371
Utilizzo di questa politica 2371
Dettagli della policy 2371
Versione della politica 2372
Documento di policy JSON 2372
Ulteriori informazioni 2379
AWSDeepRacerAccountAdminAccess 2379
Utilizzo di questa politica 2379
Dettagli della policy 2379
Versione della politica 2380
Documento di policy JSON 2380
Ulteriori informazioni 2380
AWSDeepRacerCloudFormationAccessPolicy 2381
Utilizzo di questa politica 2381
Dettagli della policy 2381
Versione della politica 2381
Documento di policy JSON 2381
Ulteriori informazioni 2384

AWSDeepRacerDefaultMultiUserAccess 2384
Utilizzo di questa politica 2384
Dettagli della policy 2385
Versione della politica 2385
Documento di policy JSON 2385
Ulteriori informazioni 2386
AWSDeepRacerFullAccess 2387
Utilizzo di questa politica 2387
Dettagli della policy 2387
Versione della politica 2387
Documento di policy JSON 2387
Ulteriori informazioni 2388
AWSDeepRacerRoboMakerAccessPolicy 2388
Utilizzo di questa politica 2389
Dettagli della policy 2389
Versione della politica 2389
Documento di policy JSON 2389
Ulteriori informazioni 2391
AWSDeepRacerServiceRolePolicy 2391
Utilizzo di questa politica 2391
Dettagli della policy 2391
Versione della politica 2392
Documento di policy JSON 2392
Ulteriori informazioni 2395
AWSDenyAll 2395
Utilizzo di questa politica 2395
Dettagli della policy 2395
Versione della politica 2396
Documento di policy JSON 2396
Ulteriori informazioni 2396
AWSDeviceFarmFullAccess 2396
Utilizzo di questa politica 2396
Dettagli della policy 2397
Versione della politica 2397
Documento di policy JSON 2397
Ulteriori informazioni 2397

AWSDeviceFarmServiceRolePolicy 2398
Utilizzo di questa politica 2398
Dettagli della policy 2398
Versione della politica 2398
Documento di policy JSON 2398
Ulteriori informazioni 2400
AWSDeviceFarmTestGridServiceRolePolicy 2400
Utilizzo di questa politica 2401
Dettagli della policy 2401
Versione della politica 2401
Documento di policy JSON 2401
Ulteriori informazioni 2403
AWSDirectConnectFullAccess 2403
Utilizzo di questa politica 2404
Dettagli della policy 2404
Versione della politica 2404
Documento di policy JSON 2404
Ulteriori informazioni 2404
AWSDirectConnectReadOnlyAccess 2405
Utilizzo di questa politica 2405
Dettagli della policy 2405
Versione della politica 2405
Documento di policy JSON 2405
Ulteriori informazioni 2406
AWSDirectConnectServiceRolePolicy 2406
Utilizzo di questa politica 2406
Dettagli della policy 2406
Versione della politica 2407
Documento di policy JSON 2407
Ulteriori informazioni 2407
AWSDirectoryServiceDataFullAccess 2407
Utilizzo di questa politica 2408
Dettagli della policy 2408
Versione della politica 2408
Documento di policy JSON 2408
Ulteriori informazioni 2409

AWSDirectoryServiceDataReadOnlyAccess 2409
Utilizzo di questa politica 2409
Dettagli della policy 2409
Versione della politica 2410
Documento di policy JSON 2410
Ulteriori informazioni 2410
AWSDirectoryServiceFullAccess 2411
Utilizzo di questa politica 2411
Dettagli della policy 2411
Versione della politica 2411
Documento di policy JSON 2411
Ulteriori informazioni 2413
AWSDirectoryServiceReadOnlyAccess 2413
Utilizzo di questa politica 2413
Dettagli della policy 2413
Versione della politica 2414
Documento di policy JSON 2414
Ulteriori informazioni 2415
AWSDirectoryServiceServiceRolePolicy 2415
Utilizzo di questa politica 2415
Dettagli della policy 2415
Versione della politica 2415
Documento di policy JSON 2415
Ulteriori informazioni 2417
AWSDiscoveryContinuousExportFirehosePolicy 2417
Utilizzo di questa politica 2417
Dettagli della policy 2417
Versione della politica 2417
Documento di policy JSON 2417
Ulteriori informazioni 2418
AWSDMSFleetAdvisorServiceRolePolicy 2419
Utilizzo di questa politica 2419
Dettagli della policy 2419
Versione della politica 2419
Documento di policy JSON 2419
Ulteriori informazioni 2420

AWSDMSServerlessServiceRolePolicy 2420
Utilizzo di questa politica 2420
Dettagli della policy 2420
Versione della politica 2420
Documento di policy JSON 2421
Ulteriori informazioni 2423
AWSEC2CapacityManagerServiceRolePolicy 2423
Utilizzo di questa politica 2424
Dettagli della policy 2424
Versione della politica 2424
Documento di policy JSON 2424
Ulteriori informazioni 2425
AWSEC2CapacityReservationFleetRolePolicy 2425
Utilizzo di questa politica 2425
Dettagli della policy 2425
Versione della politica 2426
Documento di policy JSON 2426
Ulteriori informazioni 2427
AWSEC2FleetServiceRolePolicy 2427
Utilizzo di questa politica 2427
Dettagli della policy 2427
Versione della politica 2428
Documento di policy JSON 2428
Ulteriori informazioni 2430
AWSEC2SpotFleetServiceRolePolicy 2430
Utilizzo di questa politica 2430
Dettagli della policy 2430
Versione della politica 2430
Documento di policy JSON 2431
Ulteriori informazioni 2433
AWSEC2SpotServiceRolePolicy 2433
Utilizzo di questa politica 2433
Dettagli della policy 2433
Versione della politica 2433
Documento di policy JSON 2433
Ulteriori informazioni 2435

AWSEC2SqlHaInstancePolicy 2435
Utilizzo di questa politica 2435
Dettagli della policy 2435
Versione della politica 2435
Documento di policy JSON 2436
Ulteriori informazioni 2437
AWSEC2SqlHaServiceRolePolicy 2437
Utilizzo di questa politica 2437
Dettagli della policy 2437
Versione della politica 2438
Documento di policy JSON 2438
Ulteriori informazioni 2440
AWSEC2VssRestorePolicy 2440
Utilizzo di questa politica 2440
Dettagli della policy 2440
Versione della politica 2440
Documento di policy JSON 2440
Ulteriori informazioni 2443
AWSEC2VssSnapshotPolicy 2443
Utilizzo di questa politica 2443
Dettagli della policy 2443
Versione della politica 2444
Documento di policy JSON 2444
Ulteriori informazioni 2447
AWSECRPullThroughCache_ServiceRolePolicy 2447
Utilizzo di questa politica 2447
Dettagli della policy 2447
Versione della politica 2448
Documento di policy JSON 2448
Ulteriori informazioni 2449
AWSElasticBeanstalkCustomPlatformforEC2Role 2449
Utilizzo di questa politica 2449
Dettagli della policy 2449
Versione della politica 2450
Documento di policy JSON 2450
Ulteriori informazioni 2451

AWSElasticBeanstalkEKSImageBuild 2452
Utilizzo di questa politica 2452
Dettagli della policy 2452
Versione della politica 2452
Documento di policy JSON 2452
Ulteriori informazioni 2454
AWSElasticBeanstalkEKSObservability 2454
Utilizzo di questa politica 2455
Dettagli della policy 2455
Versione della politica 2455
Documento di policy JSON 2455
Ulteriori informazioni 2457
AWSElasticBeanstalkEKSTagging 2457
Utilizzo di questa politica 2457
Dettagli della policy 2457
Versione della politica 2457
Documento di policy JSON 2458
Ulteriori informazioni 2460
AWSElasticBeanstalkEnhancedHealth 2460
Utilizzo di questa politica 2460
Dettagli della policy 2460
Versione della politica 2461
Documento di policy JSON 2461
Ulteriori informazioni 2462
AWSElasticBeanstalkMaintenance 2462
Utilizzo di questa politica 2462
Dettagli della policy 2462
Versione della politica 2463
Documento di policy JSON 2463
Ulteriori informazioni 2464
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 2464
Utilizzo di questa politica 2464
Dettagli della policy 2464
Versione della politica 2464
Documento di policy JSON 2465
Ulteriori informazioni 2472

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 2472
Utilizzo di questa politica 2472
Dettagli della policy 2472
Versione della politica 2472
Documento di policy JSON 2473
Ulteriori informazioni 2478
AWSElasticBeanstalkMulticontainerDocker 2478
Utilizzo di questa politica 2479
Dettagli della policy 2479
Versione della politica 2479
Documento di policy JSON 2479
Ulteriori informazioni 2481
AWSElasticBeanstalkReadOnly 2481
Utilizzo di questa politica 2481
Dettagli della policy 2482
Versione della politica 2482
Documento di policy JSON 2482
Ulteriori informazioni 2484
AWSElasticBeanstalkRoleCore 2485
Utilizzo di questa politica 2485
Dettagli della policy 2485
Versione della politica 2485
Documento di policy JSON 2485
Ulteriori informazioni 2490
AWSElasticBeanstalkRoleCWL 2490
Utilizzo di questa politica 2491
Dettagli della policy 2491
Versione della politica 2491
Documento di policy JSON 2491
Ulteriori informazioni 2492
AWSElasticBeanstalkRoleECS 2492
Utilizzo di questa politica 2492
Dettagli della policy 2492
Versione della politica 2492
Documento di policy JSON 2492
Ulteriori informazioni 2493

AWSElasticBeanstalkRoleRDS 2494
Utilizzo di questa politica 2494
Dettagli della policy 2494
Versione della politica 2494
Documento di policy JSON 2494
Ulteriori informazioni 2495
AWSElasticBeanstalkRoleSNS 2495
Utilizzo di questa politica 2495
Dettagli della policy 2495
Versione della politica 2495
Documento di policy JSON 2496
Ulteriori informazioni 2496
AWSElasticBeanstalkRoleWorkerTier 2497
Utilizzo di questa politica 2497
Dettagli della policy 2497
Versione della politica 2497
Documento di policy JSON 2497
Ulteriori informazioni 2498
AWSElasticBeanstalkService 2498
Utilizzo di questa politica 2498
Dettagli della policy 2498
Versione della politica 2499
Documento di policy JSON 2499
Ulteriori informazioni 2503
AWSElasticBeanstalkServiceRolePolicy 2503
Utilizzo di questa politica 2504
Dettagli della policy 2504
Versione della politica 2504
Documento sulla politica JSON 2504
Ulteriori informazioni 2518
AWSElasticBeanstalkWebTier 2518
Utilizzo di questa politica 2518
Dettagli della policy 2518
Versione della politica 2518
Documento di policy JSON 2519
Ulteriori informazioni 2521

AWSElasticBeanstalkWorkerTier 2521
Utilizzo di questa politica 2521
Dettagli della policy 2521
Versione della politica 2522
Documento di policy JSON 2522
Ulteriori informazioni 2525
AWSElasticDisasterRecoveryAgentInstallationPolicy 2525
Utilizzo di questa politica 2525
Dettagli della policy 2526
Versione della politica 2526
Documento di policy JSON 2526
Ulteriori informazioni 2527
AWSElasticDisasterRecoveryAgentPolicy 2528
Utilizzo di questa politica 2528
Dettagli della policy 2528
Versione della politica 2528
Documento di policy JSON 2528
Ulteriori informazioni 2529
AWSElasticDisasterRecoveryConsoleFullAccess 2529
Utilizzo di questa politica 2530
Dettagli della policy 2530
Versione della politica 2530
Documento di policy JSON 2530
Ulteriori informazioni 2540
AWSElasticDisasterRecoveryConsoleFullAccess_v2 2540
Utilizzo di questa politica 2541
Dettagli della policy 2541
Versione della politica 2541
Documento di policy JSON 2541
Ulteriori informazioni 2557
AWSElasticDisasterRecoveryConversionServerPolicy 2557
Utilizzo di questa politica 2557
Dettagli della policy 2557
Versione della politica 2558
Documento di policy JSON 2558
Ulteriori informazioni 2558

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 2559
Utilizzo di questa politica 2559
Dettagli della policy 2559
Versione della politica 2559
Documento di policy JSON 2559
Ulteriori informazioni 2560
AWSElasticDisasterRecoveryEc2InstancePolicy 2560
Utilizzo di questa politica 2561
Dettagli della policy 2561
Versione della politica 2561
Documento di policy JSON 2561
Ulteriori informazioni 2563
AWSElasticDisasterRecoveryFailbackInstallationPolicy 2563
Utilizzo di questa politica 2563
Dettagli della policy 2564
Versione della politica 2564
Documento di policy JSON 2564
Ulteriori informazioni 2565
AWSElasticDisasterRecoveryFailbackPolicy 2565
Utilizzo di questa politica 2565
Dettagli della policy 2565
Versione della politica 2566
Documento sulla politica JSON 2566
Ulteriori informazioni 2567
AWSElasticDisasterRecoveryLaunchActionsPolicy 2567
Utilizzo di questa politica 2567
Dettagli della policy 2568
Versione della politica 2568
Documento di policy JSON 2568
Ulteriori informazioni 2574
AWSElasticDisasterRecoveryNetworkReplicationPolicy 2574
Utilizzo di questa politica 2574
Dettagli della policy 2575
Versione della politica 2575
Documento di policy JSON 2575
Ulteriori informazioni 2576

AWSElasticDisasterRecoveryReadOnlyAccess 2576
Utilizzo di questa politica 2576
Dettagli della policy 2576
Versione della politica 2576
Documento di policy JSON 2577
Ulteriori informazioni 2579
AWSElasticDisasterRecoveryRecoveryInstancePolicy 2579
Utilizzo di questa politica 2579
Dettagli della policy 2579
Versione della politica 2580
Documento di policy JSON 2580
Ulteriori informazioni 2582
AWSElasticDisasterRecoveryReplicationServerPolicy 2582
Utilizzo di questa politica 2583
Dettagli della policy 2583
Versione della politica 2583
Documento di policy JSON 2583
Ulteriori informazioni 2585
AWSElasticDisasterRecoveryServiceRolePolicy 2586
Utilizzo di questa politica 2586
Dettagli della policy 2586
Versione della politica 2586
Documento di policy JSON 2586
Ulteriori informazioni 2596
AWSElasticDisasterRecoveryStagingAccountPolicy 2596
Utilizzo di questa politica 2597
Dettagli della policy 2597
Versione della politica 2597
Documento di policy JSON 2597
Ulteriori informazioni 2598
AWSElasticDisasterRecoveryStagingAccountPolicy_v2 2598
Utilizzo di questa politica 2598
Dettagli della policy 2599
Versione della politica 2599
Documento di policy JSON 2599
Ulteriori informazioni 2600

AWSElasticLoadBalancingClassicServiceRolePolicy 2600
Utilizzo di questa politica 2600
Dettagli della policy 2601
Versione della politica 2601
Documento di policy JSON 2601
Ulteriori informazioni 2602
AWSElasticLoadBalancingServiceRolePolicy 2602
Utilizzo di questa politica 2602
Dettagli della policy 2602
Versione della politica 2602
Documento di policy JSON 2603
Ulteriori informazioni 2604
AWSElementalMediaConnectCreateBridge 2604
Utilizzo di questa politica 2604
Dettagli della policy 2604
Versione della politica 2604
Documento di policy JSON 2605
Ulteriori informazioni 2605
AWSElementalMediaConnectCreateFlow 2605
Utilizzo di questa politica 2606
Dettagli della policy 2606
Versione della politica 2606
Documento di policy JSON 2606
Ulteriori informazioni 2607
AWSElementalMediaConnectDeleteBridge 2607
Utilizzo di questa politica 2607
Dettagli della policy 2607
Versione della politica 2608
Documento di policy JSON 2608
Ulteriori informazioni 2608
AWSElementalMediaConnectDeleteFlow 2609
Utilizzo di questa politica 2609
Dettagli della policy 2609
Versione della politica 2609
Documento di policy JSON 2609
Ulteriori informazioni 2610

AWSElementalMediaConnectFullAccess 2610
Utilizzo di questa politica 2610
Dettagli della policy 2610
Versione della politica 2611
Documento di policy JSON 2611
Ulteriori informazioni 2611
AWSElementalMediaConnectReadOnlyAccess 2611
Utilizzo di questa politica 2612
Dettagli della policy 2612
Versione della politica 2612
Documento di policy JSON 2612
Ulteriori informazioni 2613
AWSElementalMediaConvertFullAccess 2613
Utilizzo di questa politica 2613
Dettagli della policy 2613
Versione della politica 2613
Documento di policy JSON 2614
Ulteriori informazioni 2614
AWSElementalMediaConvertReadOnly 2615
Utilizzo di questa politica 2615
Dettagli della policy 2615
Versione della politica 2615
Documento di policy JSON 2615
Ulteriori informazioni 2616
AWSElementalMediaLiveFullAccess 2616
Utilizzo di questa politica 2616
Dettagli della policy 2616
Versione della politica 2616
Documento di policy JSON 2617
Ulteriori informazioni 2617
AWSElementalMediaLiveReadOnly 2617
Utilizzo di questa politica 2617
Dettagli della policy 2617
Versione della politica 2618
Documento di policy JSON 2618
Ulteriori informazioni 2618

AWSElementalMediaPackageFullAccess 2618
Utilizzo di questa politica 2619
Dettagli della policy 2619
Versione della politica 2619
Documento di policy JSON 2619
Ulteriori informazioni 2619
AWSElementalMediaPackageReadOnly 2620
Utilizzo di questa politica 2620
Dettagli della policy 2620
Versione della politica 2620
Documento di policy JSON 2620
Ulteriori informazioni 2621
AWSElementalMediaPackageV2FullAccess 2621
Utilizzo di questa politica 2621
Dettagli della policy 2621
Versione della politica 2621
Documento di policy JSON 2621
Ulteriori informazioni 2622
AWSElementalMediaPackageV2ReadOnly 2622
Utilizzo di questa politica 2622
Dettagli della policy 2622
Versione della politica 2622
Documento di policy JSON 2623
Ulteriori informazioni 2623
AWSElementalMediaStoreFullAccess 2623
Utilizzo di questa politica 2623
Dettagli della policy 2623
Versione della politica 2624
Documento di policy JSON 2624
Ulteriori informazioni 2624
AWSElementalMediaStoreReadOnly 2624
Utilizzo di questa politica 2625
Dettagli della policy 2625
Versione della politica 2625
Documento di policy JSON 2625
Ulteriori informazioni 2626

AWSElementalMediaTailorFullAccess 2626
Utilizzo di questa politica 2626
Dettagli della policy 2626
Versione della politica 2626
Documento di policy JSON 2626
Ulteriori informazioni 2627
AWSElementalMediaTailorReadOnly 2627
Utilizzo di questa politica 2627
Dettagli della policy 2627
Versione della politica 2627
Documento di policy JSON 2628
Ulteriori informazioni 2628
AWSEnhancedClassicNetworkingMangementPolicy 2628
Utilizzo di questa politica 2628
Dettagli della policy 2628
Versione della politica 2629
Documento di policy JSON 2629
Ulteriori informazioni 2629
AWSEntityResolutionConsoleFullAccess 2629
Utilizzo di questa politica 2630
Dettagli della policy 2630
Versione della politica 2630
Documento di policy JSON 2630
Ulteriori informazioni 2633
AWSEntityResolutionConsoleReadOnlyAccess 2633
Utilizzo di questa politica 2634
Dettagli della policy 2634
Versione della politica 2634
Documento di policy JSON 2634
Ulteriori informazioni 2635
AWSFaultInjectionSimulatorEC2Access 2635
Utilizzo di questa politica 2635
Dettagli della policy 2635
Versione della politica 2635
Documento di policy JSON 2635
Ulteriori informazioni 2637

AWSFaultInjectionSimulatorECSAccess 2637
Utilizzo di questa politica 2637
Dettagli della policy 2638
Versione della politica 2638
Documento di policy JSON 2638
Ulteriori informazioni 2640
AWSFaultInjectionSimulatorEKSAccess 2640
Utilizzo di questa politica 2641
Dettagli della policy 2641
Versione della politica 2641
Documento di policy JSON 2641
Ulteriori informazioni 2642
AWSFaultInjectionSimulatorNetworkAccess 2642
Utilizzo di questa politica 2643
Dettagli della policy 2643
Versione della politica 2643
Documento di policy JSON 2643
Ulteriori informazioni 2650
AWSFaultInjectionSimulatorRDSAccess 2650
Utilizzo di questa politica 2650
Dettagli della policy 2650
Versione della politica 2651
Documento di policy JSON 2651
Ulteriori informazioni 2652
AWSFaultInjectionSimulatorSSMAccess 2652
Utilizzo di questa politica 2652
Dettagli della policy 2652
Versione della politica 2653
Documento di policy JSON 2653
Ulteriori informazioni 2654
AWSFinSpaceServiceRolePolicy 2654
Utilizzo di questa politica 2655
Dettagli della policy 2655
Versione della politica 2655
Documento di policy JSON 2655
Ulteriori informazioni 2656

AWSFMAdminFullAccess 2656
Utilizzo di questa politica 2656
Dettagli della policy 2656
Versione della politica 2656
Documento di policy JSON 2656
Ulteriori informazioni 2658
AWSFMAdminReadOnlyAccess 2658
Utilizzo di questa politica 2659
Dettagli della policy 2659
Versione della politica 2659
Documento di policy JSON 2659
Ulteriori informazioni 2661
AWSFMMemberReadOnlyAccess 2661
Utilizzo di questa politica 2661
Dettagli della policy 2661
Versione della politica 2661
Documento di policy JSON 2661
Ulteriori informazioni 2662
AWSForWordPressPluginPolicy 2662
Utilizzo di questa politica 2662
Dettagli della policy 2662
Versione della politica 2663
Documento di policy JSON 2663
Ulteriori informazioni 2665
AWSGitSyncServiceRolePolicy 2665
Utilizzo di questa politica 2665
Dettagli della policy 2665
Versione della politica 2665
Documento di policy JSON 2665
Ulteriori informazioni 2666
AWSGlobalAcceleratorSLRPolicy 2666
Utilizzo di questa politica 2666
Dettagli della policy 2667
Versione della politica 2667
Documento di policy JSON 2667
Ulteriori informazioni 2669

AWSGlueConsoleFullAccess 2669
Utilizzo di questa politica 2669
Dettagli della policy 2669
Versione della politica 2669
Documento di policy JSON 2669
Ulteriori informazioni 2673
AWSGlueConsoleSageMakerNotebookFullAccess 2674
Utilizzo di questa politica 2674
Dettagli della policy 2674
Versione della politica 2674
Documento di policy JSON 2674
Ulteriori informazioni 2680
AwsGlueDataBrewFullAccessPolicy 2680
Utilizzo di questa politica 2680
Dettagli della policy 2680
Versione della politica 2680
Documento di policy JSON 2680
Ulteriori informazioni 2686
AWSGlueDataBrewServiceRole 2686
Utilizzo di questa politica 2686
Dettagli della policy 2686
Versione della politica 2686
Documento di policy JSON 2687
Ulteriori informazioni 2689
AWSGlueSchemaRegistryFullAccess 2690
Utilizzo di questa politica 2690
Dettagli della policy 2690
Versione della politica 2690
Documento di policy JSON 2690
Ulteriori informazioni 2691
AWSGlueSchemaRegistryReadonlyAccess 2692
Utilizzo di questa politica 2692
Dettagli della policy 2692
Versione della politica 2692
Documento di policy JSON 2692
Ulteriori informazioni 2693

AWSGlueServiceNotebookRole 2693
Utilizzo di questa politica 2693
Dettagli della policy 2693
Versione della politica 2694
Documento di policy JSON 2694
Ulteriori informazioni 2696
AWSGlueServiceRole 2696
Utilizzo di questa politica 2696
Dettagli della policy 2697
Versione della politica 2697
Documento di policy JSON 2697
Ulteriori informazioni 2699
AwsGlueSessionUserRestrictedNotebookPolicy 2699
Utilizzo di questa politica 2700
Dettagli della policy 2700
Versione della politica 2700
Documento di policy JSON 2700
Ulteriori informazioni 2703
AwsGlueSessionUserRestrictedNotebookServiceRole 2703
Utilizzo di questa politica 2703
Dettagli della policy 2703
Versione della politica 2704
Documento di policy JSON 2704
Ulteriori informazioni 2708
AwsGlueSessionUserRestrictedPolicy 2708
Utilizzo di questa politica 2708
Dettagli della policy 2708
Versione della politica 2708
Documento di policy JSON 2709
Ulteriori informazioni 2711
AwsGlueSessionUserRestrictedServiceRole 2712
Utilizzo di questa politica 2712
Dettagli della policy 2712
Versione della politica 2712
Documento di policy JSON 2712
Ulteriori informazioni 2717

AWSGrafanaAccountAdministrator 2717
Utilizzo di questa politica 2717
Dettagli della policy 2717
Versione della politica 2717
Documento di policy JSON 2718
Ulteriori informazioni 2719
AWSGrafanaConsoleReadOnlyAccess 2719
Utilizzo di questa politica 2719
Dettagli della policy 2719
Versione della politica 2719
Documento di policy JSON 2719
Ulteriori informazioni 2720
AWSGrafanaWorkspacePermissionManagement 2720
Utilizzo di questa politica 2720
Dettagli della policy 2720
Versione della politica 2721
Documento di policy JSON 2721
Ulteriori informazioni 2722
AWSGrafanaWorkspacePermissionManagementV2 2722
Utilizzo di questa politica 2722
Dettagli della policy 2722
Versione della politica 2722
Documento di policy JSON 2723
Ulteriori informazioni 2723
AWSGreengrassFullAccess 2724
Utilizzo di questa politica 2724
Dettagli della policy 2724
Versione della politica 2724
Documento di policy JSON 2724
Ulteriori informazioni 2725
AWSGreengrassReadOnlyAccess 2725
Utilizzo di questa politica 2725
Dettagli della policy 2725
Versione della politica 2725
Documento di policy JSON 2726
Ulteriori informazioni 2726

AWSGreengrassResourceAccessRolePolicy 2726
Utilizzo di questa politica 2726
Dettagli della policy 2726
Versione della politica 2727
Documento di policy JSON 2727
Ulteriori informazioni 2729
AWSGroundStationAgentInstancePolicy 2729
Utilizzo di questa politica 2730
Dettagli della policy 2730
Versione della politica 2730
Documento di policy JSON 2730
Ulteriori informazioni 2731
AWSHealth_EventProcessorServiceRolePolicy 2731
Utilizzo di questa politica 2731
Dettagli della policy 2731
Versione della politica 2731
Documento di policy JSON 2731
Ulteriori informazioni 2732
AWSHealthFullAccess 2732
Utilizzo di questa politica 2733
Dettagli della policy 2733
Versione della politica 2733
Documento di policy JSON 2733
Ulteriori informazioni 2734
AWSHealthImagingFullAccess 2734
Utilizzo di questa politica 2734
Dettagli della policy 2735
Versione della politica 2735
Documento di policy JSON 2735
Ulteriori informazioni 2736
AWSHealthImagingReadOnlyAccess 2736
Utilizzo di questa politica 2736
Dettagli della policy 2736
Versione della politica 2736
Documento di policy JSON 2736
Ulteriori informazioni 2737

AWSHealthImagingServiceRolePolicy 2737
Utilizzo di questa politica 2737
Dettagli della policy 2738
Versione della politica 2738
Documento di policy JSON 2738
Ulteriori informazioni 2738
AWSHealthOmicsServiceLinkedRolePolicy 2739
Utilizzo di questa politica 2739
Dettagli della policy 2739
Versione della politica 2739
Documento di policy JSON 2739
Ulteriori informazioni 2741
AWSIAMIdentityCenterAllowListForIdentityContext 2742
Utilizzo di questa politica 2742
Dettagli della policy 2742
Versione della politica 2742
Documento di policy JSON 2742
Ulteriori informazioni 2745
AWSIAMRoleManagerServiceRolePolicy 2746
Utilizzo di questa politica 2746
Dettagli della policy 2746
Versione della politica 2746
Documento sulla politica JSON 2746
Ulteriori informazioni 2747
AWSIdentityCenterExternalManagementPolicy 2747
Utilizzo di questa politica 2747
Dettagli della policy 2747
Versione della politica 2747
Documento di policy JSON 2748
Ulteriori informazioni 2749
AWSIdentitySyncFullAccess 2749
Utilizzo di questa politica 2750
Dettagli della policy 2750
Versione della politica 2750
Documento di policy JSON 2750
Ulteriori informazioni 2751

AWSIdentitySyncReadOnlyAccess 2751
Utilizzo di questa politica 2751
Dettagli della policy 2751
Versione della politica 2752
Documento di policy JSON 2752
Ulteriori informazioni 2752
AWSImageBuilderFullAccess 2752
Utilizzo di questa politica 2753
Dettagli della policy 2753
Versione della politica 2753
Documento di policy JSON 2753
Ulteriori informazioni 2756
AWSImageBuilderReadOnlyAccess 2756
Utilizzo di questa politica 2756
Dettagli della policy 2756
Versione della politica 2756
Documento di policy JSON 2757
Ulteriori informazioni 2757
AWSImportExportFullAccess 2757
Utilizzo di questa politica 2757
Dettagli della policy 2758
Versione della politica 2758
Documento di policy JSON 2758
Ulteriori informazioni 2758
AWSImportExportReadOnlyAccess 2759
Utilizzo di questa politica 2759
Dettagli della policy 2759
Versione della politica 2759
Documento di policy JSON 2759
Ulteriori informazioni 2760
AWSIncidentManagerIncidentAccessServiceRolePolicy 2760
Utilizzo di questa politica 2760
Dettagli della policy 2760
Versione della politica 2760
Documento di policy JSON 2761
Ulteriori informazioni 2761

AWSIncidentManagerResolverAccess 2761
Utilizzo di questa politica 2761
Dettagli della policy 2762
Versione della politica 2762
Documento di policy JSON 2762
Ulteriori informazioni 2763
AWSIncidentManagerServiceRolePolicy 2763
Utilizzo di questa politica 2763
Dettagli della policy 2763
Versione della politica 2764
Documento di policy JSON 2764
Ulteriori informazioni 2765
AWSIoT1ClickFullAccess 2765
Utilizzo di questa politica 2765
Dettagli della policy 2765
Versione della politica 2766
Documento di policy JSON 2766
Ulteriori informazioni 2766
AWSIoT1ClickReadOnlyAccess 2766
Utilizzo di questa politica 2767
Dettagli della policy 2767
Versione della politica 2767
Documento di policy JSON 2767
Ulteriori informazioni 2767
AWSIoTAnalyticsFullAccess 2768
Utilizzo di questa politica 2768
Dettagli della policy 2768
Versione della politica 2768
Documento di policy JSON 2768
Ulteriori informazioni 2769
AWSIoTAnalyticsReadOnlyAccess 2769
Utilizzo di questa politica 2769
Dettagli della policy 2769
Versione della politica 2769
Documento di policy JSON 2770
Ulteriori informazioni 2770

AWSIoTConfigAccess 2770
Utilizzo di questa politica 2770
Dettagli della policy 2770
Versione della politica 2771
Documento di policy JSON 2771
Ulteriori informazioni 2775
AWSIoTConfigReadOnlyAccess 2775
Utilizzo di questa politica 2775
Dettagli della policy 2775
Versione della politica 2775
Documento di policy JSON 2775
Ulteriori informazioni 2777
AWSIoTDataAccess 2778
Utilizzo di questa politica 2778
Dettagli della policy 2778
Versione della politica 2778
Documento di policy JSON 2778
Ulteriori informazioni 2779
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 2779
Utilizzo di questa politica 2779
Dettagli della policy 2779
Versione della politica 2780
Documento di policy JSON 2780
Ulteriori informazioni 2780
AWSIoTDeviceDefenderAudit 2780
Utilizzo di questa politica 2781
Dettagli della policy 2781
Versione della politica 2781
Documento di policy JSON 2781
Ulteriori informazioni 2782
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 2782
Utilizzo di questa politica 2782
Dettagli della policy 2782
Versione della politica 2783
Documento di policy JSON 2783
Ulteriori informazioni 2784

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 2784
Utilizzo di questa politica 2784
Dettagli della policy 2784
Versione della politica 2784
Documento di policy JSON 2785
Ulteriori informazioni 2785
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 2785
Utilizzo di questa politica 2785
Dettagli della policy 2786
Versione della politica 2786
Documento di policy JSON 2786
Ulteriori informazioni 2786
AWSIoTDeviceDefenderUpdateCACertMitigationAction 2787
Utilizzo di questa politica 2787
Dettagli della policy 2787
Versione della politica 2787
Documento di policy JSON 2787
Ulteriori informazioni 2788
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 2788
Utilizzo di questa politica 2788
Dettagli della policy 2788
Versione della politica 2789
Documento di policy JSON 2789
Ulteriori informazioni 2789
AWSIoTDeviceTesterForFreeRTOSFullAccess 2789
Utilizzo di questa politica 2790
Dettagli della policy 2790
Versione della politica 2790
Documento di policy JSON 2790
Ulteriori informazioni 2796
AWSIoTDeviceTesterForGreengrassFullAccess 2796
Utilizzo di questa politica 2797
Dettagli della policy 2797
Versione della politica 2797
Documento di policy JSON 2797
Ulteriori informazioni 2800

AWSIoTEventsFullAccess 2800
Utilizzo di questa politica 2800
Dettagli della policy 2800
Versione della politica 2801
Documento di policy JSON 2801
Ulteriori informazioni 2801
AWSIoTEventsReadOnlyAccess 2801
Utilizzo di questa politica 2801
Dettagli della policy 2802
Versione della politica 2802
Documento di policy JSON 2802
Ulteriori informazioni 2802
AWSIoTFleetHubFederationAccess 2803
Utilizzo di questa politica 2803
Dettagli della policy 2803
Versione della politica 2803
Documento di policy JSON 2803
Ulteriori informazioni 2805
AWSIoTFleetwiseServiceRolePolicy 2805
Utilizzo di questa politica 2805
Dettagli della policy 2805
Versione della politica 2806
Documento di policy JSON 2806
Ulteriori informazioni 2806
AWSIoTFullAccess 2807
Utilizzo di questa politica 2807
Dettagli della policy 2807
Versione della politica 2807
Documento di policy JSON 2807
Ulteriori informazioni 2808
AWSIoTLogging 2808
Utilizzo di questa politica 2808
Dettagli della policy 2808
Versione della politica 2808
Documento di policy JSON 2809
Ulteriori informazioni 2809

AWSIoTManagedIntegrationsFullAccess 2809
Utilizzo di questa politica 2809
Dettagli della policy 2810
Versione della politica 2810
Documento di policy JSON 2810
Ulteriori informazioni 2811
AWSIoTManagedIntegrationsRolePolicy 2811
Utilizzo di questa politica 2811
Dettagli della policy 2811
Versione della politica 2811
Documento di policy JSON 2812
Ulteriori informazioni 2813
AWSIoTOTAUpdate 2813
Utilizzo di questa politica 2813
Dettagli della policy 2813
Versione della politica 2813
Documento di policy JSON 2814
Ulteriori informazioni 2814
AWSIotRoboRunnerFullAccess 2814
Utilizzo di questa politica 2814
Dettagli della policy 2814
Versione della politica 2815
Documento di policy JSON 2815
Ulteriori informazioni 2815
AWSIotRoboRunnerReadOnly 2816
Utilizzo di questa politica 2816
Dettagli della policy 2816
Versione della politica 2816
Documento di policy JSON 2816
Ulteriori informazioni 2817
AWSIotRoboRunnerServiceRolePolicy 2817
Utilizzo di questa politica 2817
Dettagli della policy 2817
Versione della politica 2818
Documento di policy JSON 2818
Ulteriori informazioni 2818

AWSIoTRuleActions 2818
Utilizzo di questa politica 2819
Dettagli della policy 2819
Versione della politica 2819
Documento di policy JSON 2819
Ulteriori informazioni 2820
AWSIoTSiteWiseConsoleFullAccess 2820
Utilizzo di questa politica 2820
Dettagli della policy 2820
Versione della politica 2820
Documento di policy JSON 2821
Ulteriori informazioni 2823
AWSIoTSiteWiseFullAccess 2823
Utilizzo di questa politica 2823
Dettagli della policy 2823
Versione della politica 2823
Documento di policy JSON 2824
Ulteriori informazioni 2824
AWSIoTSiteWiseMonitorPortalAccess 2824
Utilizzo di questa politica 2824
Dettagli della policy 2824
Versione della politica 2825
Documento di policy JSON 2825
Ulteriori informazioni 2826
AWSIoTSiteWiseMonitorServiceRolePolicy 2826
Utilizzo di questa politica 2826
Dettagli della policy 2826
Versione della politica 2827
Documento di policy JSON 2827
Ulteriori informazioni 2828
AWSIoTSiteWiseReadOnlyAccess 2828
Utilizzo di questa politica 2828
Dettagli della policy 2828
Versione della politica 2828
Documento di policy JSON 2828
Ulteriori informazioni 2830

AWSIoTThingsRegistration 2830
Utilizzo di questa politica 2830
Dettagli della policy 2831
Versione della politica 2831
Documento di policy JSON 2831
Ulteriori informazioni 2832
AWSIoTTwinMakerServiceRolePolicy 2832
Utilizzo di questa politica 2832
Dettagli della policy 2833
Versione della politica 2833
Documento di policy JSON 2833
Ulteriori informazioni 2835
AWSIoTWirelessDataAccess 2835
Utilizzo di questa politica 2835
Dettagli della policy 2835
Versione della politica 2835
Documento di policy JSON 2835
Ulteriori informazioni 2836
AWSIoTWirelessFullAccess 2836
Utilizzo di questa politica 2836
Dettagli della policy 2836
Versione della politica 2836
Documento di policy JSON 2837
Ulteriori informazioni 2837
AWSIoTWirelessFullPublishAccess 2837
Utilizzo di questa politica 2837
Dettagli della policy 2838
Versione della politica 2838
Documento di policy JSON 2838
Ulteriori informazioni 2838
AWSIoTWirelessGatewayCertManager 2839
Utilizzo di questa politica 2839
Dettagli della policy 2839
Versione della politica 2839
Documento di policy JSON 2839
Ulteriori informazioni 2840

AWSIoTWirelessLogging 2840
Utilizzo di questa politica 2840
Dettagli della policy 2840
Versione della politica 2840
Documento di policy JSON 2841
Ulteriori informazioni 2841
AWSIoTWirelessReadOnlyAccess 2841
Utilizzo di questa politica 2841
Dettagli della policy 2841
Versione della politica 2842
Documento di policy JSON 2842
Ulteriori informazioni 2842
AWSIPAMServiceRolePolicy 2843
Utilizzo di questa politica 2843
Dettagli della policy 2843
Versione della politica 2843
Documento di policy JSON 2843
Ulteriori informazioni 2845
AWSIQContractServiceRolePolicy 2845
Utilizzo di questa politica 2846
Dettagli della policy 2846
Versione della politica 2846
Documento di policy JSON 2846
Ulteriori informazioni 2846
AWSIQFullAccess 2847
Utilizzo di questa politica 2847
Dettagli della policy 2847
Versione della politica 2847
Documento di policy JSON 2847
Ulteriori informazioni 2848
AWSIQPermissionServiceRolePolicy 2848
Utilizzo di questa politica 2848
Dettagli della policy 2848
Versione della politica 2849
Documento di policy JSON 2849
Ulteriori informazioni 2850

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 2850
Utilizzo di questa politica 2850
Dettagli della policy 2850
Versione della politica 2850
Documento di policy JSON 2851
Ulteriori informazioni 2851
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 2851
Utilizzo di questa politica 2851
Dettagli della policy 2852
Versione della politica 2852
Documento di policy JSON 2852
Ulteriori informazioni 2852
AWSKeyManagementServicePowerUser 2853
Utilizzo di questa politica 2853
Dettagli della policy 2853
Versione della politica 2853
Documento di policy JSON 2853
Ulteriori informazioni 2854
AWSLakeFormationCrossAccountManager 2854
Utilizzo di questa politica 2854
Dettagli della policy 2854
Versione della politica 2855
Documento di policy JSON 2855
Ulteriori informazioni 2857
AWSLakeFormationDataAdmin 2857
Utilizzo di questa politica 2857
Dettagli della policy 2857
Versione della politica 2857
Documento di policy JSON 2858
Ulteriori informazioni 2859
AWSLambda_FullAccess 2859
Utilizzo di questa politica 2859
Dettagli della policy 2859
Versione della politica 2860
Documento di policy JSON 2860
Ulteriori informazioni 2861

AWSLambda_ReadOnlyAccess 2862
Utilizzo di questa politica 2862
Dettagli della policy 2862
Versione della politica 2862
Documento di policy JSON 2862
Ulteriori informazioni 2864
AWSLambdaBasicDurableExecutionRolePolicy 2864
Utilizzo di questa politica 2864
Dettagli della policy 2864
Versione della politica 2864
Documento di policy JSON 2865
Ulteriori informazioni 2865
AWSLambdaBasicExecutionRole 2865
Utilizzo di questa politica 2865
Dettagli della policy 2865
Versione della politica 2866
Documento di policy JSON 2866
Ulteriori informazioni 2866
AWSLambdaDynamoDBExecutionRole 2867
Utilizzo di questa politica 2867
Dettagli della policy 2867
Versione della politica 2867
Documento di policy JSON 2867
Ulteriori informazioni 2868
AWSLambdaENIManagementAccess 2868
Utilizzo di questa politica 2868
Dettagli della policy 2868
Versione della politica 2868
Documento di policy JSON 2869
Ulteriori informazioni 2869
AWSLambdaExecute 2869
Utilizzo di questa politica 2870
Dettagli della policy 2870
Versione della politica 2870
Documento di policy JSON 2870
Ulteriori informazioni 2871

AWSLambdaFullAccess 2871
Utilizzo di questa politica 2871
Dettagli della policy 2871
Versione della politica 2872
Documento di policy JSON 2872
Ulteriori informazioni 2873
AWSLambdaInvocation-DynamoDB 2873
Utilizzo di questa politica 2874
Dettagli della policy 2874
Versione della politica 2874
Documento di policy JSON 2874
Ulteriori informazioni 2875
AWSLambdaKinesisExecutionRole 2875
Utilizzo di questa politica 2875
Dettagli della policy 2875
Versione della politica 2875
Documento di policy JSON 2876
Ulteriori informazioni 2876
AWSLambdaManagedEC2ResourceOperator 2876
Utilizzo di questa politica 2877
Dettagli della policy 2877
Versione della politica 2877
Documento di policy JSON 2877
Ulteriori informazioni 2879
AWSLambdaMSKExecutionRole 2879
Utilizzo di questa politica 2879
Dettagli della policy 2879
Versione della politica 2880
Documento di policy JSON 2880
Ulteriori informazioni 2880
AWSLambdaNetworkConnectorOperatorPolicy 2881
Utilizzo di questa politica 2881
Dettagli della policy 2881
Versione della politica 2881
Documento di policy JSON 2881
Ulteriori informazioni 2882

AWSLambdaReplicator 2883
Utilizzo di questa politica 2883
Dettagli della policy 2883
Versione della politica 2883
Documento di policy JSON 2883
Ulteriori informazioni 2884
AWSLambdaRole 2885
Utilizzo di questa politica 2885
Dettagli della policy 2885
Versione della politica 2885
Documento di policy JSON 2885
Ulteriori informazioni 2886
AWSLambdaServiceRolePolicy 2886
Utilizzo di questa politica 2886
Dettagli della policy 2886
Versione della politica 2886
Documento di policy JSON 2887
Ulteriori informazioni 2888
AWSLambdaSQSQueueExecutionRole 2888
Utilizzo di questa politica 2888
Dettagli della policy 2888
Versione della politica 2888
Documento di policy JSON 2889
Ulteriori informazioni 2889
AWSLambdaVPCAccessExecutionRole 2889
Utilizzo di questa politica 2889
Dettagli della policy 2890
Versione della politica 2890
Documento di policy JSON 2890
Ulteriori informazioni 2891
AWSLicenseManagerConsumptionPolicy 2891
Utilizzo di questa politica 2891
Dettagli della policy 2891
Versione della politica 2891
Documento di policy JSON 2891
Ulteriori informazioni 2892

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 2892
Utilizzo di questa politica 2892
Dettagli della policy 2892
Versione della politica 2893
Documento di policy JSON 2893
Ulteriori informazioni 2895
AWSLicenseManagerMasterAccountRolePolicy 2895
Utilizzo di questa politica 2895
Dettagli della policy 2895
Versione della politica 2895
Documento di policy JSON 2895
Ulteriori informazioni 2900
AWSLicenseManagerMemberAccountRolePolicy 2900
Utilizzo di questa politica 2901
Dettagli della policy 2901
Versione della politica 2901
Documento di policy JSON 2901
Ulteriori informazioni 2902
AWSLicenseManagerServiceRolePolicy 2902
Utilizzo di questa politica 2903
Dettagli della policy 2903
Versione della politica 2903
Documento di policy JSON 2903
Ulteriori informazioni 2907
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 2907
Utilizzo di questa politica 2907
Dettagli della policy 2907
Versione della politica 2907
Documento di policy JSON 2907
Ulteriori informazioni 2911
AWSM2ServicePolicy 2911
Utilizzo di questa politica 2911
Dettagli della policy 2911
Versione della politica 2911
Documento di policy JSON 2911
Ulteriori informazioni 2913

AWSManagedAccountManagementAccess 2913
Utilizzo di questa politica 2913
Dettagli della policy 2913
Versione della politica 2913
Documento sulla politica JSON 2914
Ulteriori informazioni 2914
AWSManagedAccountUserEntitlementAccess 2914
Utilizzo di questa politica 2915
Dettagli della policy 2915
Versione della politica 2915
Documento sulla politica JSON 2915
Ulteriori informazioni 2916
AWSManagedAdvancedFeaturesActivationAccess 2916
Utilizzo di questa politica 2916
Dettagli della policy 2916
Versione della politica 2916
Documento sulla politica JSON 2917
Ulteriori informazioni 2917
AWSManagedBudgetsSpendLimitManagementAccess 2917
Utilizzo di questa politica 2917
Dettagli della policy 2917
Versione della politica 2918
Documento sulla politica JSON 2918
Ulteriori informazioni 2919
AWSManagedControlPolicyManagementAccess 2919
Utilizzo di questa politica 2919
Dettagli della policy 2919
Versione della politica 2919
Documento sulla politica JSON 2920
Ulteriori informazioni 2920
AWSManagedServiceAccessManagementAccess 2920
Utilizzo di questa politica 2921
Dettagli della policy 2921
Versione della politica 2921
Documento sulla politica JSON 2921
Ulteriori informazioni 2923

AWSManagedServices_ContactsServiceRolePolicy 2923
Utilizzo di questa politica 2923
Dettagli della policy 2923
Versione della politica 2924
Documento di policy JSON 2924
Ulteriori informazioni 2925
AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 2925
Utilizzo di questa politica 2925
Dettagli della policy 2925
Versione della politica 2925
Documento di policy JSON 2925
Ulteriori informazioni 2927
AWSManagedServices_EventsServiceRolePolicy 2927
Utilizzo di questa politica 2927
Dettagli della policy 2927
Versione della politica 2928
Documento di policy JSON 2928
Ulteriori informazioni 2928
AWSManagedServices_SelfServiceReporting_ServiceRolePolicy 2929
Utilizzo di questa politica 2929
Dettagli della policy 2929
Versione della politica 2929
Documento di policy JSON 2929
Ulteriori informazioni 2930
AWSManagedServicesDeploymentToolkitPolicy 2930
Utilizzo di questa politica 2930
Dettagli della policy 2930
Versione della politica 2931
Documento di policy JSON 2931
Ulteriori informazioni 2933
AWSManagedSettingsAdminAccess 2933
Utilizzo di questa politica 2933
Dettagli della policy 2933
Versione della politica 2934
Documento sulla politica JSON 2934
Ulteriori informazioni 2942

AWSManagedSettingsReadOnlyAccess 2942
Utilizzo di questa politica 2942
Dettagli della policy 2943
Versione della politica 2943
Documento sulla politica JSON 2943
Ulteriori informazioni 2944
AWSManagedSignUpAdminAccess 2944
Utilizzo di questa politica 2945
Dettagli della policy 2945
Versione della politica 2945
Documento sulla politica JSON 2945
Ulteriori informazioni 2947
AWSManagementConsoleAdministratorAccess 2947
Utilizzo di questa politica 2947
Dettagli della policy 2947
Versione della politica 2948
Documento di policy JSON 2948
Ulteriori informazioni 2950
AWSManagementConsoleBasicUserAccess 2950
Utilizzo di questa politica 2950
Dettagli della policy 2950
Versione della politica 2951
Documento di policy JSON 2951
Ulteriori informazioni 2952
AWSMarketplaceAmiIngestion 2952
Utilizzo di questa politica 2952
Dettagli della policy 2952
Versione della politica 2953
Documento di policy JSON 2953
Ulteriori informazioni 2953
AWSMarketplaceDeploymentServiceRolePolicy 2954
Utilizzo di questa politica 2954
Dettagli della policy 2954
Versione della politica 2954
Documento di policy JSON 2954
Ulteriori informazioni 2956

AWSMarketplaceDiscoveryFullAccess 2956
Utilizzo di questa politica 2956
Dettagli della policy 2956
Versione della politica 2956
Documento di policy JSON 2957
Ulteriori informazioni 2957
AWSMarketplaceFullAccess 2958
Utilizzo di questa politica 2958
Dettagli della policy 2958
Versione della politica 2958
Documento di policy JSON 2958
Ulteriori informazioni 2960
AWSMarketplaceGetEntitlements 2960
Utilizzo di questa politica 2960
Dettagli della policy 2960
Versione della politica 2961
Documento di policy JSON 2961
Ulteriori informazioni 2961
AWSMarketplaceImageBuildFullAccess 2962
Utilizzo di questa politica 2962
Dettagli della policy 2962
Versione della politica 2962
Documento di policy JSON 2962
Ulteriori informazioni 2966
AWSMarketplaceLicenseManagementServiceRolePolicy 2966
Utilizzo di questa politica 2966
Dettagli della policy 2966
Versione della politica 2966
Documento di policy JSON 2967
Ulteriori informazioni 2967
AWSMarketplaceManageSubscriptions 2967
Utilizzo di questa politica 2968
Dettagli della policy 2968
Versione della politica 2968
Documento di policy JSON 2968
Ulteriori informazioni 2971

AWSMarketplaceMeteringFullAccess 2971
Utilizzo di questa politica 2972
Dettagli della policy 2972
Versione della politica 2972
Documento di policy JSON 2972
Ulteriori informazioni 2972
AWSMarketplaceMeteringRegisterUsage 2973
Utilizzo di questa politica 2973
Dettagli della policy 2973
Versione della politica 2973
Documento di policy JSON 2973
Ulteriori informazioni 2974
AWSMarketplaceProcurementSystemAdminFullAccess 2974
Utilizzo di questa politica 2974
Dettagli della policy 2974
Versione della politica 2974
Documento di policy JSON 2975
Ulteriori informazioni 2975
AWSMarketplacePurchaseOrdersServiceRolePolicy 2975
Utilizzo di questa politica 2976
Dettagli della policy 2976
Versione della politica 2976
Documento di policy JSON 2976
Ulteriori informazioni 2977
AWSMarketplaceRead-only 2977
Utilizzo di questa politica 2977
Dettagli della policy 2977
Versione della politica 2977
Documento di policy JSON 2977
Ulteriori informazioni 2979
AWSMarketplaceResaleAuthorizationServiceRolePolicy 2979
Utilizzo di questa politica 2980
Dettagli della policy 2980
Versione della politica 2980
Documento di policy JSON 2980
Ulteriori informazioni 2982

AWSMarketplaceSellerFullAccess 2983
Utilizzo di questa politica 2983
Dettagli della policy 2983
Versione della politica 2983
Documento sulla politica JSON 2983
Ulteriori informazioni 2990
AWSMarketplaceSellerOfferManagement 2990
Utilizzo di questa politica 2991
Dettagli della policy 2991
Versione della politica 2991
Documento di policy JSON 2991
Ulteriori informazioni 2994
AWSMarketplaceSellerProductsFullAccess 2994
Utilizzo di questa politica 2994
Dettagli della policy 2994
Versione della politica 2994
Documento di policy JSON 2994
Ulteriori informazioni 2998
AWSMarketplaceSellerProductsReadOnly 2998
Utilizzo di questa politica 2998
Dettagli della policy 2998
Versione della politica 2998
Documento di policy JSON 2999
Ulteriori informazioni 2999
AWSMcpServiceActionsFullAccess 3000
Utilizzo di questa politica 3000
Dettagli della policy 3000
Versione della politica 3000
Documento di policy JSON 3000
Ulteriori informazioni 3001
AWSMCPSignInOAuthAccessPolicy 3001
Utilizzo di questa politica 3001
Dettagli della policy 3001
Versione della politica 3001
Documento di policy JSON 3002
Ulteriori informazioni 3002

AWSMediaConnectServicePolicy 3002
Utilizzo di questa politica 3002
Dettagli della policy 3003
Versione della politica 3003
Documento di policy JSON 3003
Ulteriori informazioni 3005
AWSMediaLiveAnywhereServiceRolePolicy 3005
Utilizzo di questa politica 3005
Dettagli della policy 3005
Versione della politica 3005
Documento di policy JSON 3006
Ulteriori informazioni 3009
AWSMediaTailorServiceRolePolicy 3009
Utilizzo di questa politica 3009
Dettagli della policy 3009
Versione della politica 3009
Documento di policy JSON 3009
Ulteriori informazioni 3010
AWSMigrationHubDiscoveryAccess 3010
Utilizzo di questa politica 3010
Dettagli della policy 3010
Versione della politica 3011
Documento di policy JSON 3011
Ulteriori informazioni 3012
AWSMigrationHubDMSAccess 3012
Utilizzo di questa politica 3012
Dettagli della policy 3013
Versione della politica 3013
Documento di policy JSON 3013
Ulteriori informazioni 3014
AWSMigrationHubFullAccess 3014
Utilizzo di questa politica 3014
Dettagli della policy 3014
Versione della politica 3015
Documento di policy JSON 3015
Ulteriori informazioni 3016

AWSMigrationHubOrchestratorConsoleFullAccess 3016
Utilizzo di questa politica 3017
Dettagli della policy 3017
Versione della politica 3017
Documento di policy JSON 3017
Ulteriori informazioni 3020
AWSMigrationHubOrchestratorInstanceRolePolicy 3020
Utilizzo di questa politica 3021
Dettagli della policy 3021
Versione della politica 3021
Documento di policy JSON 3021
Ulteriori informazioni 3022
AWSMigrationHubOrchestratorPlugin 3022
Utilizzo di questa politica 3022
Dettagli della policy 3022
Versione della politica 3022
Documento di policy JSON 3023
Ulteriori informazioni 3024
AWSMigrationHubOrchestratorServiceRolePolicy 3024
Utilizzo di questa politica 3024
Dettagli della policy 3024
Versione della politica 3025
Documento di policy JSON 3025
Ulteriori informazioni 3028
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 3029
Utilizzo di questa politica 3029
Dettagli della policy 3029
Versione della politica 3029
Documento di policy JSON 3029
Ulteriori informazioni 3035
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 3035
Utilizzo di questa politica 3035
Dettagli della policy 3036
Versione della politica 3036
Documento di policy JSON 3036
Ulteriori informazioni 3037

AWSMigrationHubRefactorSpacesFullAccess 3038
Utilizzo di questa politica 3038
Dettagli della policy 3038
Versione della politica 3038
Documento di policy JSON 3038
Ulteriori informazioni 3045
AWSMigrationHubRefactorSpacesServiceRolePolicy 3045
Utilizzo di questa politica 3045
Dettagli della policy 3045
Versione della politica 3046
Documento di policy JSON 3046
Ulteriori informazioni 3049
AWSMigrationHubSMSAccess 3050
Utilizzo di questa politica 3050
Dettagli della policy 3050
Versione della politica 3050
Documento di policy JSON 3050
Ulteriori informazioni 3051
AWSMigrationHubStrategyCollector 3051
Utilizzo di questa politica 3052
Dettagli della policy 3052
Versione della politica 3052
Documento di policy JSON 3052
Ulteriori informazioni 3054
AWSMigrationHubStrategyConsoleFullAccess 3055
Utilizzo di questa politica 3055
Dettagli della policy 3055
Versione della politica 3055
Documento di policy JSON 3055
Ulteriori informazioni 3057
AWSMigrationHubStrategyServiceRolePolicy 3057
Utilizzo di questa politica 3057
Dettagli della policy 3057
Versione della politica 3058
Documento di policy JSON 3058
Ulteriori informazioni 3059

AWSMobileHub_FullAccess 3059
Utilizzo di questa politica 3059
Dettagli della policy 3059
Versione della politica 3059
Documento di policy JSON 3060
Ulteriori informazioni 3061
AWSMobileHub_ReadOnly 3061
Utilizzo di questa politica 3062
Dettagli della policy 3062
Versione della politica 3062
Documento di policy JSON 3062
Ulteriori informazioni 3063
AWSMSKReplicatorExecutionRole 3063
Utilizzo di questa politica 3064
Dettagli della policy 3064
Versione della politica 3064
Documento di policy JSON 3064
Ulteriori informazioni 3065
AWSNATGatewayServiceRolePolicy 3066
Utilizzo di questa politica 3066
Dettagli della policy 3066
Versione della politica 3066
Documento di policy JSON 3066
Ulteriori informazioni 3067
AWSNetworkFirewallFullAccess 3067
Utilizzo di questa politica 3067
Dettagli della policy 3067
Versione della politica 3068
Documento di policy JSON 3068
Ulteriori informazioni 3072
AWSNetworkFirewallReadOnlyAccess 3072
Utilizzo di questa politica 3072
Dettagli della policy 3072
Versione della politica 3072
Documento di policy JSON 3073
Ulteriori informazioni 3074

AWSNetworkFirewallServiceRolePolicy 3074
Utilizzo di questa politica 3074
Dettagli della policy 3074
Versione della politica 3074
Documento di policy JSON 3075
Ulteriori informazioni 3076
AWSNetworkManagerCloudWANServiceRolePolicy 3077
Utilizzo di questa politica 3077
Dettagli della policy 3077
Versione della politica 3077
Documento di policy JSON 3077
Ulteriori informazioni 3078
AWSNetworkManagerFullAccess 3078
Utilizzo di questa politica 3078
Dettagli della policy 3078
Versione della politica 3078
Documento di policy JSON 3079
Ulteriori informazioni 3079
AWSNetworkManagerReadOnlyAccess 3079
Utilizzo di questa politica 3080
Dettagli della policy 3080
Versione della politica 3080
Documento di policy JSON 3080
Ulteriori informazioni 3080
AWSNetworkManagerServiceRolePolicy 3081
Utilizzo di questa politica 3081
Dettagli della policy 3081
Versione della politica 3081
Documento di policy JSON 3081
Ulteriori informazioni 3082
AWSObservabilityAdminLogsCentralizationServiceRolePolicy 3083
Utilizzo di questa politica 3083
Dettagli della policy 3083
Versione della politica 3083
Documento di policy JSON 3083
Ulteriori informazioni 3084

AWSObservabilityAdminServiceRolePolicy 3084
Utilizzo di questa politica 3085
Dettagli della policy 3085
Versione della politica 3085
Documento sulla politica JSON 3085
Ulteriori informazioni 3088
AWSObservabilityAdminTelemetryEnablementServiceRolePolicy 3088
Utilizzo di questa politica 3088
Dettagli della policy 3088
Versione della politica 3088
Documento sulla politica JSON 3089
Ulteriori informazioni 3102
AWSOrganizationsFullAccess 3102
Utilizzo di questa politica 3102
Dettagli della policy 3103
Versione della politica 3103
Documento di policy JSON 3103
Ulteriori informazioni 3104
AWSOrganizationsReadOnlyAccess 3104
Utilizzo di questa politica 3104
Dettagli della policy 3104
Versione della politica 3105
Documento di policy JSON 3105
Ulteriori informazioni 3106
AWSOrganizationsServiceTrustPolicy 3106
Utilizzo di questa politica 3106
Dettagli della policy 3106
Versione della politica 3106
Documento di policy JSON 3107
Ulteriori informazioni 3107
AWSOutpostsAuthorizeServerPolicy 3107
Utilizzo di questa politica 3108
Dettagli della policy 3108
Versione della politica 3108
Documento di policy JSON 3108
Ulteriori informazioni 3108

AWSOutpostsServiceRolePolicy 3109
Utilizzo di questa politica 3109
Dettagli della policy 3109
Versione della politica 3109
Documento di policy JSON 3109
Ulteriori informazioni 3111
AWSPanoramaApplianceRolePolicy 3111
Utilizzo di questa politica 3111
Dettagli della policy 3112
Versione della politica 3112
Documento di policy JSON 3112
Ulteriori informazioni 3113
AWSPanoramaApplianceServiceRolePolicy 3113
Utilizzo di questa politica 3113
Dettagli della policy 3113
Versione della politica 3113
Documento di policy JSON 3114
Ulteriori informazioni 3115
AWSPanoramaFullAccess 3115
Utilizzo di questa politica 3115
Dettagli della policy 3115
Versione della politica 3116
Documento di policy JSON 3116
Ulteriori informazioni 3118
AWSPanoramaGreengrassGroupRolePolicy 3119
Utilizzo di questa politica 3119
Dettagli della policy 3119
Versione della politica 3119
Documento di policy JSON 3119
Ulteriori informazioni 3121
AWSPanoramaSageMakerRolePolicy 3121
Utilizzo di questa politica 3121
Dettagli della policy 3121
Versione della politica 3121
Documento di policy JSON 3122
Ulteriori informazioni 3122

AWSPanoramaServiceLinkedRolePolicy 3122
Utilizzo di questa politica 3122
Dettagli della policy 3123
Versione della politica 3123
Documento di policy JSON 3123
Ulteriori informazioni 3126
AWSPanoramaServiceRolePolicy 3126
Utilizzo di questa politica 3126
Dettagli della policy 3126
Versione della politica 3126
Documento di policy JSON 3126
Ulteriori informazioni 3133
AWSPartnerCentralChannelHandshakeApprovalManagement 3134
Utilizzo di questa politica 3134
Dettagli della policy 3134
Versione della politica 3134
Documento di policy JSON 3134
Ulteriori informazioni 3135
AWSPartnerCentralChannelManagement 3135
Utilizzo di questa politica 3135
Dettagli della policy 3135
Versione della politica 3136
Documento di policy JSON 3136
Ulteriori informazioni 3139
AWSPartnerCentralFullAccess 3139
Utilizzo di questa politica 3139
Dettagli della policy 3139
Versione della politica 3139
Documento di policy JSON 3139
Ulteriori informazioni 3144
AWSPartnerCentralMarketingManagement 3144
Utilizzo di questa politica 3144
Dettagli della policy 3144
Versione della politica 3144
Documento di policy JSON 3145
Ulteriori informazioni 3147

AWSPartnerCentralOpportunityManagement 3147
Utilizzo di questa politica 3147
Dettagli della policy 3148
Versione della politica 3148
Documento di policy JSON 3148
Ulteriori informazioni 3152
AWSPartnerCentralRevenueAttributionManagement 3152
Utilizzo di questa politica 3153
Dettagli della policy 3153
Versione della politica 3153
Documento di policy JSON 3153
Ulteriori informazioni 3158
AWSPartnerCentralSandboxFullAccess 3158
Utilizzo di questa politica 3158
Dettagli della policy 3158
Versione della politica 3158
Documento di policy JSON 3159
Ulteriori informazioni 3160
AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy 3160
Utilizzo di questa politica 3160
Dettagli della policy 3160
Versione della politica 3161
Documento di policy JSON 3161
Ulteriori informazioni 3161
AWSPartnerLedSupportReadOnlyAccess 3162
Utilizzo di questa politica 3162
Dettagli della policy 3162
Versione della politica 3162
Documento di policy JSON 3162
Ulteriori informazioni 3199
AWSPartnerProServeToolsFullAccess 3199
Utilizzo di questa politica 3200
Dettagli della policy 3200
Versione della politica 3200
Documento di policy JSON 3200
Ulteriori informazioni 3201

AWSPartnerProServeToolsIndividualContributor 3201
Utilizzo di questa politica 3201
Dettagli della policy 3201
Versione della politica 3201
Documento di policy JSON 3202
Ulteriori informazioni 3202
AWSPartnerProServeToolsOrganizationReaderIndividualContributor 3202
Utilizzo di questa politica 3203
Dettagli della policy 3203
Versione della politica 3203
Documento di policy JSON 3203
Ulteriori informazioni 3204
AWSPCSComputeNodePolicy 3204
Utilizzo di questa politica 3204
Dettagli della policy 3204
Versione della politica 3204
Documento di policy JSON 3205
Ulteriori informazioni 3205
AWSPCSServiceRolePolicy 3205
Utilizzo di questa politica 3205
Dettagli della policy 3205
Versione della politica 3206
Documento di policy JSON 3206
Ulteriori informazioni 3211
AWSPriceListServiceFullAccess 3211
Utilizzo di questa politica 3211
Dettagli della policy 3211
Versione della politica 3211
Documento di policy JSON 3212
Ulteriori informazioni 3212
AWSPrivateCAAuditor 3212
Utilizzo di questa politica 3212
Dettagli della policy 3212
Versione della politica 3213
Documento di policy JSON 3213
Ulteriori informazioni 3214

AWSPrivateCAConnectorForKubernetesPolicy 3214
Utilizzo di questa politica 3214
Dettagli della policy 3214
Versione della politica 3214
Documento di policy JSON 3214
Ulteriori informazioni 3215
AWSPrivateCAFullAccess 3215
Utilizzo di questa politica 3215
Dettagli della policy 3215
Versione della politica 3216
Documento di policy JSON 3216
Ulteriori informazioni 3216
AWSPrivateCAPrivilegedUser 3216
Utilizzo di questa politica 3217
Dettagli della policy 3217
Versione della politica 3217
Documento di policy JSON 3217
Ulteriori informazioni 3218
AWSPrivateCAReadOnly 3218
Utilizzo di questa politica 3219
Dettagli della policy 3219
Versione della politica 3219
Documento di policy JSON 3219
Ulteriori informazioni 3220
AWSPrivateCAUser 3220
Utilizzo di questa politica 3220
Dettagli della policy 3220
Versione della politica 3220
Documento di policy JSON 3220
Ulteriori informazioni 3222
AWSPrivateMarketplaceAdminFullAccess 3222
Utilizzo di questa politica 3222
Dettagli della policy 3222
Versione della politica 3222
Documento di policy JSON 3223
Ulteriori informazioni 3225

AWSPrivateMarketplaceRequests 3226
Utilizzo di questa politica 3226
Dettagli della policy 3226
Versione della politica 3226
Documento di policy JSON 3226
Ulteriori informazioni 3228
AWSPrivateNetworksServiceRolePolicy 3228
Utilizzo di questa politica 3228
Dettagli della policy 3228
Versione della politica 3229
Documento di policy JSON 3229
Ulteriori informazioni 3229
AWSProtonCodeBuildProvisioningBasicAccess 3230
Utilizzo di questa politica 3230
Dettagli della policy 3230
Versione della politica 3230
Documento di policy JSON 3230
Ulteriori informazioni 3231
AWSProtonCodeBuildProvisioningServiceRolePolicy 3231
Utilizzo di questa politica 3231
Dettagli della policy 3231
Versione della politica 3232
Documento di policy JSON 3232
Ulteriori informazioni 3233
AWSProtonDeveloperAccess 3233
Utilizzo di questa politica 3233
Dettagli della policy 3233
Versione della politica 3234
Documento di policy JSON 3234
Ulteriori informazioni 3236
AWSProtonFullAccess 3236
Utilizzo di questa politica 3237
Dettagli della policy 3237
Versione della politica 3237
Documento di policy JSON 3237
Ulteriori informazioni 3239

AWSProtonReadOnlyAccess 3239
Utilizzo di questa politica 3239
Dettagli della policy 3240
Versione della politica 3240
Documento di policy JSON 3240
Ulteriori informazioni 3241
AWSProtonServiceGitSyncServiceRolePolicy 3242
Utilizzo di questa politica 3242
Dettagli della policy 3242
Versione della politica 3242
Documento di policy JSON 3242
Ulteriori informazioni 3243
AWSProtonSyncServiceRolePolicy 3243
Utilizzo di questa politica 3243
Dettagli della policy 3243
Versione della politica 3244
Documento di policy JSON 3244
Ulteriori informazioni 3245
AWSPurchaseOrdersServiceRolePolicy 3245
Utilizzo di questa politica 3245
Dettagli della policy 3245
Versione della politica 3246
Documento di policy JSON 3246
Ulteriori informazioni 3247
AWSQuickSetupCFGCPacksPermissionsBoundary 3247
Utilizzo di questa politica 3247
Dettagli della policy 3247
Versione della politica 3247
Documento di policy JSON 3248
Ulteriori informazioni 3250
AWSQuickSetupDeploymentRolePolicy 3251
Utilizzo di questa politica 3251
Dettagli della policy 3251
Versione della politica 3251
Documento di policy JSON 3251
Ulteriori informazioni 3259

AWSQuickSetupDevOpsGuruPermissionsBoundary 3260
Utilizzo di questa politica 3260
Dettagli della policy 3260
Versione della politica 3260
Documento di policy JSON 3260
Ulteriori informazioni 3263
AWSQuickSetupDistributorPermissionsBoundary 3263
Utilizzo di questa politica 3264
Dettagli della policy 3264
Versione della politica 3264
Documento di policy JSON 3264
Ulteriori informazioni 3270
AWSQuickSetupEnableAREXExecutionPolicy 3270
Utilizzo di questa politica 3270
Dettagli della policy 3270
Versione della politica 3270
Documento di policy JSON 3271
Ulteriori informazioni 3272
AWSQuickSetupEnableDHMCExecutionPolicy 3272
Utilizzo di questa politica 3273
Dettagli della policy 3273
Versione della politica 3273
Documento di policy JSON 3273
Ulteriori informazioni 3274
AWSQuickSetupJITNADeploymentRolePolicy 3275
Utilizzo di questa politica 3275
Dettagli della policy 3275
Versione della politica 3275
Documento di policy JSON 3275
Ulteriori informazioni 3279
AWSQuickSetupManagedInstanceProfileExecutionPolicy 3279
Utilizzo di questa politica 3279
Dettagli della policy 3279
Versione della politica 3279
Documento di policy JSON 3280
Ulteriori informazioni 3284

AWSQuickSetupManageJITNAResourcesExecutionPolicy 3285
Utilizzo di questa politica 3285
Dettagli della policy 3285
Versione della politica 3285
Documento di policy JSON 3285
Ulteriori informazioni 3287
AWSQuickSetupPatchPolicyBaselineAccess 3288
Utilizzo di questa politica 3288
Dettagli della policy 3288
Versione della politica 3288
Documento di policy JSON 3288
Ulteriori informazioni 3289
AWSQuickSetupPatchPolicyDeploymentRolePolicy 3289
Utilizzo di questa politica 3290
Dettagli della policy 3290
Versione della politica 3290
Documento di policy JSON 3290
Ulteriori informazioni 3298
AWSQuickSetupPatchPolicyLambdaExecutionPolicy 3298
Utilizzo di questa politica 3298
Dettagli della policy 3298
Versione della politica 3299
Documento di policy JSON 3299
Ulteriori informazioni 3300
AWSQuickSetupPatchPolicyPermissionsBoundary 3300
Utilizzo di questa politica 3300
Dettagli della policy 3300
Versione della politica 3300
Documento di policy JSON 3301
Ulteriori informazioni 3309
AWSQuickSetupPatchPolicyTagManagementExecutionPolicy 3309
Utilizzo di questa politica 3309
Dettagli della policy 3309
Versione della politica 3310
Documento di policy JSON 3310
Ulteriori informazioni 3311

AWSQuickSetupSchedulerPermissionsBoundary 3311
Utilizzo di questa politica 3311
Dettagli della policy 3311
Versione della politica 3312
Documento di policy JSON 3312
Ulteriori informazioni 3315
AWSQuickSetupSSMDeploymentRolePolicy 3315
Utilizzo di questa politica 3315
Dettagli della policy 3316
Versione della politica 3316
Documento di policy JSON 3316
Ulteriori informazioni 3327
AWSQuickSetupSSMDeploymentS3BucketRolePolicy 3327
Utilizzo di questa politica 3327
Dettagli della policy 3327
Versione della politica 3327
Documento di policy JSON 3328
Ulteriori informazioni 3328
AWSQuickSetupSSMHostMgmtPermissionsBoundary 3329
Utilizzo di questa politica 3329
Dettagli della policy 3329
Versione della politica 3329
Documento di policy JSON 3329
Ulteriori informazioni 3335
AWSQuickSetupSSMLifecycleManagementExecutionPolicy 3335
Utilizzo di questa politica 3336
Dettagli della policy 3336
Versione della politica 3336
Documento di policy JSON 3336
Ulteriori informazioni 3337
AWSQuickSetupSSMManageResourcesExecutionPolicy 3338
Utilizzo di questa politica 3338
Dettagli della policy 3338
Versione della politica 3338
Documento di policy JSON 3338
Ulteriori informazioni 3341

AWSQuickSetupStartSSMAssociationsExecutionPolicy 3341
Utilizzo di questa politica 3341
Dettagli della policy 3342
Versione della politica 3342
Documento di policy JSON 3342
Ulteriori informazioni 3343
AWSQuickSetupStartStopInstancesExecutionPolicy 3343
Utilizzo di questa politica 3343
Dettagli della policy 3344
Versione della politica 3344
Documento di policy JSON 3344
Ulteriori informazioni 3346
AWSQuickSightAssetBundleExportPolicy 3346
Utilizzo di questa politica 3346
Dettagli della policy 3346
Versione della politica 3346
Documento di policy JSON 3346
Ulteriori informazioni 3349
AWSQuickSightAssetBundleImportPolicy 3349
Utilizzo di questa politica 3349
Dettagli della policy 3349
Versione della politica 3349
Documento di policy JSON 3349
Ulteriori informazioni 3352
AWSQuicksightAthenaAccess 3353
Utilizzo di questa politica 3353
Dettagli della policy 3353
Versione della politica 3353
Documento di policy JSON 3353
Ulteriori informazioni 3355
AWSQuickSightDescribeRDS 3356
Utilizzo di questa politica 3356
Dettagli della policy 3356
Versione della politica 3356
Documento di policy JSON 3356
Ulteriori informazioni 3357

AWSQuickSightDescribeRedshift 3357
Utilizzo di questa politica 3357
Dettagli della policy 3357
Versione della politica 3357
Documento di policy JSON 3358
Ulteriori informazioni 3358
AWSQuickSightElasticsearchPolicy 3358
Utilizzo di questa politica 3358
Dettagli della policy 3358
Versione della politica 3359
Documento di policy JSON 3359
Ulteriori informazioni 3360
AWSQuickSightIoTAnalyticsAccess 3360
Utilizzo di questa politica 3360
Dettagli della policy 3360
Versione della politica 3361
Documento di policy JSON 3361
Ulteriori informazioni 3361
AWSQuickSightListIAM 3361
Utilizzo di questa politica 3362
Dettagli della policy 3362
Versione della politica 3362
Documento di policy JSON 3362
Ulteriori informazioni 3362
AWSQuicksightOpenSearchPolicy 3363
Utilizzo di questa politica 3363
Dettagli della policy 3363
Versione della politica 3363
Documento di policy JSON 3363
Ulteriori informazioni 3364
AWSQuickSightSageMakerPolicy 3365
Utilizzo di questa politica 3365
Dettagli della policy 3365
Versione della politica 3365
Documento di policy JSON 3365
Ulteriori informazioni 3366

AWSQuickSightSecretsManagerWriteAccess 3367
Utilizzo di questa politica 3367
Dettagli della policy 3367
Versione della politica 3367
Documento di policy JSON 3367
Ulteriori informazioni 3368
AWSQuickSightSecretsManagerWritePolicy 3368
Utilizzo di questa politica 3369
Dettagli della policy 3369
Versione della politica 3369
Documento di policy JSON 3369
Ulteriori informazioni 3370
AWSQuickSightTimestreamPolicy 3370
Utilizzo di questa politica 3370
Dettagli della policy 3370
Versione della politica 3371
Documento di policy JSON 3371
Ulteriori informazioni 3371
AWSReachabilityAnalyzerServiceRolePolicy 3372
Utilizzo di questa politica 3372
Dettagli della policy 3372
Versione della politica 3372
Documento di policy JSON 3372
Ulteriori informazioni 3374
AWSRefactoringToolkitFullAccess 3375
Utilizzo di questa politica 3375
Dettagli della policy 3375
Versione della politica 3375
Documento di policy JSON 3375
Ulteriori informazioni 3389
AWSRefactoringToolkitSidecarPolicy 3389
Utilizzo di questa politica 3389
Dettagli della policy 3389
Versione della politica 3390
Documento di policy JSON 3390
Ulteriori informazioni 3391

AWSrePostPrivateCloudWatchAccess 3391
Utilizzo di questa politica 3391
Dettagli della policy 3391
Versione della politica 3391
Documento di policy JSON 3392
Ulteriori informazioni 3392
AWSRepostSpaceSupportOperationsPolicy 3392
Utilizzo di questa politica 3393
Dettagli della policy 3393
Versione della politica 3393
Documento di policy JSON 3393
Ulteriori informazioni 3394
AWSResilienceHubAsssessmentExecutionPolicy 3394
Utilizzo di questa politica 3394
Dettagli della policy 3394
Versione della politica 3394
Documento di policy JSON 3395
Ulteriori informazioni 3399
AWSResilienceHubResilienceTestingPolicy 3400
Utilizzo di questa politica 3400
Dettagli della policy 3400
Versione della politica 3400
Documento sulla politica JSON 3400
Ulteriori informazioni 3403
AWSResilienceHubServiceRolePolicy 3403
Utilizzo di questa politica 3404
Dettagli della policy 3404
Versione della politica 3404
Documento di policy JSON 3404
Ulteriori informazioni 3405
AWSResilienceHubV2AssessmentExecutionPolicy 3405
Utilizzo di questa politica 3405
Dettagli della policy 3405
Versione della politica 3405
Documento di policy JSON 3406
Ulteriori informazioni 3412

AWSResourceAccessManagerFullAccess 3412
Utilizzo di questa politica 3412
Dettagli della policy 3412
Versione della politica 3412
Documento di policy JSON 3412
Ulteriori informazioni 3413
AWSResourceAccessManagerReadOnlyAccess 3413
Utilizzo di questa politica 3413
Dettagli della policy 3413
Versione della politica 3413
Documento di policy JSON 3414
Ulteriori informazioni 3414
AWSResourceAccessManagerResourceShareParticipantAccess 3414
Utilizzo di questa politica 3414
Dettagli della policy 3415
Versione della politica 3415
Documento di policy JSON 3415
Ulteriori informazioni 3416
AWSResourceAccessManagerServiceRolePolicy 3416
Utilizzo di questa politica 3416
Dettagli della policy 3416
Versione della politica 3416
Documento di policy JSON 3417
Ulteriori informazioni 3417
AWSResourceExplorerFullAccess 3418
Utilizzo di questa politica 3418
Dettagli della policy 3418
Versione della politica 3418
Documento di policy JSON 3418
Ulteriori informazioni 3419
AWSResourceExplorerOrganizationsAccess 3419
Utilizzo di questa politica 3420
Dettagli della policy 3420
Versione della politica 3420
Documento di policy JSON 3420
Ulteriori informazioni 3422

AWSResourceExplorerReadOnlyAccess 3422
Utilizzo di questa politica 3422
Dettagli della policy 3422
Versione della politica 3422
Documento di policy JSON 3423
Ulteriori informazioni 3423
AWSResourceExplorerServiceRolePolicy 3423
Utilizzo di questa politica 3424
Dettagli della policy 3424
Versione della politica 3424
Documento sulla politica JSON 3424
Ulteriori informazioni 3448
AWSResourceGroupsReadOnlyAccess 3448
Utilizzo di questa politica 3448
Dettagli della policy 3449
Versione della politica 3449
Documento di policy JSON 3449
Ulteriori informazioni 3450
AWSRevenueAttributionManagement 3451
Utilizzo di questa politica 3451
Dettagli della policy 3451
Versione della politica 3451
Documento di policy JSON 3451
Ulteriori informazioni 3453
AWSRoboMaker_FullAccess 3453
Utilizzo di questa politica 3453
Dettagli della policy 3453
Versione della politica 3454
Documento di policy JSON 3454
Ulteriori informazioni 3455
AWSRoboMakerReadOnlyAccess 3455
Utilizzo di questa politica 3455
Dettagli della policy 3456
Versione della politica 3456
Documento di policy JSON 3456
Ulteriori informazioni 3456

AWSRoboMakerServicePolicy 3457
Utilizzo di questa politica 3457
Dettagli della policy 3457
Versione della politica 3457
Documento di policy JSON 3457
Ulteriori informazioni 3459
AWSRoboMakerServiceRolePolicy 3459
Utilizzo di questa politica 3459
Dettagli della policy 3459
Versione della politica 3459
Documento di policy JSON 3460
Ulteriori informazioni 3461
AWSRolesAnywhereFullAccess 3461
Utilizzo di questa politica 3461
Dettagli della policy 3461
Versione della politica 3462
Documento di policy JSON 3462
Ulteriori informazioni 3464
AWSRolesAnywhereReadOnly 3464
Utilizzo di questa politica 3465
Dettagli della policy 3465
Versione della politica 3465
Documento di policy JSON 3465
Ulteriori informazioni 3467
AWSRolesAnywhereServicePolicy 3467
Utilizzo di questa politica 3467
Dettagli della policy 3467
Versione della politica 3467
Documento di policy JSON 3468
Ulteriori informazioni 3468
AWSS3OnOutpostsServiceRolePolicy 3468
Utilizzo di questa politica 3469
Dettagli della policy 3469
Versione della politica 3469
Documento di policy JSON 3469
Ulteriori informazioni 3472

AWSSavingsPlansFullAccess 3472
Utilizzo di questa politica 3472
Dettagli della policy 3472
Versione della politica 3472
Documento di policy JSON 3473
Ulteriori informazioni 3473
AWSSavingsPlansReadOnlyAccess 3473
Utilizzo di questa politica 3473
Dettagli della policy 3473
Versione della politica 3474
Documento di policy JSON 3474
Ulteriori informazioni 3474
AWSSDMPServiceRolePolicy 3474
Utilizzo di questa politica 3475
Dettagli della policy 3475
Versione della politica 3475
Documento sulla politica JSON 3475
Ulteriori informazioni 3478
AWSSecretsManagerClientReadOnlyAccess 3478
Utilizzo di questa politica 3478
Dettagli della policy 3479
Versione della politica 3479
Documento di policy JSON 3479
Ulteriori informazioni 3480
AWSSecurityAgentServiceRolePolicy 3480
Utilizzo di questa politica 3480
Dettagli della policy 3480
Versione della politica 3481
Documento di policy JSON 3481
Ulteriori informazioni 3483
AWSSecurityAgentWebAppPolicy 3483
Utilizzo di questa politica 3483
Dettagli della policy 3483
Versione della politica 3483
Documento di policy JSON 3484
Ulteriori informazioni 3486

AWSSecurityHubFullAccess 3486
Utilizzo di questa politica 3486
Dettagli della policy 3486
Versione della politica 3486
Documento di policy JSON 3487
Ulteriori informazioni 3488
AWSSecurityHubOrganizationsAccess 3488
Utilizzo di questa politica 3488
Dettagli della policy 3489
Versione della politica 3489
Documento di policy JSON 3489
Ulteriori informazioni 3491
AWSSecurityHubReadOnlyAccess 3492
Utilizzo di questa politica 3492
Dettagli della policy 3492
Versione della politica 3492
Documento di policy JSON 3492
Ulteriori informazioni 3493
AWSSecurityHubServiceRolePolicy 3493
Utilizzo di questa politica 3493
Dettagli della policy 3493
Versione della politica 3493
Documento di policy JSON 3494
Ulteriori informazioni 3497
AWSSecurityHubV2ServiceRolePolicy 3497
Utilizzo di questa politica 3497
Dettagli della policy 3497
Versione della politica 3497
Documento di policy JSON 3497
Ulteriori informazioni 3503
AWSSecurityIncidentResponseCaseFullAccess 3504
Utilizzo di questa politica 3504
Dettagli della policy 3504
Versione della politica 3504
Documento di policy JSON 3504
Ulteriori informazioni 3505

AWSSecurityIncidentResponseFullAccess 3505
Utilizzo di questa politica 3506
Dettagli della policy 3506
Versione della politica 3506
Documento di policy JSON 3506
Ulteriori informazioni 3508
AWSSecurityIncidentResponseReadOnlyAccess 3508
Utilizzo di questa politica 3508
Dettagli della policy 3508
Versione della politica 3508
Documento di policy JSON 3509
Ulteriori informazioni 3509
AWSSecurityIncidentResponseServiceRolePolicy 3509
Utilizzo di questa politica 3510
Dettagli della policy 3510
Versione della politica 3510
Documento di policy JSON 3510
Ulteriori informazioni 3511
AWSSecurityIncidentResponseTriageServiceRolePolicy 3512
Utilizzo di questa politica 3512
Dettagli della policy 3512
Versione della politica 3512
Documento di policy JSON 3512
Ulteriori informazioni 3515
AWSServiceCatalogAdminFullAccess 3515
Utilizzo di questa politica 3515
Dettagli della policy 3515
Versione della politica 3515
Documento di policy JSON 3515
Ulteriori informazioni 3518
AWSServiceCatalogAdminReadOnlyAccess 3518
Utilizzo di questa politica 3518
Dettagli della policy 3519
Versione della politica 3519
Documento di policy JSON 3519
Ulteriori informazioni 3520

AWSServiceCatalogAppRegistryFullAccess 3520
Utilizzo di questa politica 3521
Dettagli della policy 3521
Versione della politica 3521
Documento di policy JSON 3521
Ulteriori informazioni 3523
AWSServiceCatalogAppRegistryReadOnlyAccess 3523
Utilizzo di questa politica 3524
Dettagli della policy 3524
Versione della politica 3524
Documento di policy JSON 3524
Ulteriori informazioni 3525
AWSServiceCatalogAppRegistryServiceRolePolicy 3525
Utilizzo di questa politica 3525
Dettagli della policy 3525
Versione della politica 3525
Documento di policy JSON 3526
Ulteriori informazioni 3527
AWSServiceCatalogEndUserFullAccess 3527
Utilizzo di questa politica 3527
Dettagli della policy 3527
Versione della politica 3527
Documento di policy JSON 3528
Ulteriori informazioni 3530
AWSServiceCatalogEndUserReadOnlyAccess 3530
Utilizzo di questa politica 3530
Dettagli della policy 3530
Versione della politica 3530
Documento di policy JSON 3531
Ulteriori informazioni 3532
AWSServiceCatalogOrgsDataSyncServiceRolePolicy 3532
Utilizzo di questa politica 3533
Dettagli della policy 3533
Versione della politica 3533
Documento di policy JSON 3533
Ulteriori informazioni 3534

AWSServiceCatalogSyncServiceRolePolicy 3534
Utilizzo di questa politica 3534
Dettagli della policy 3534
Versione della politica 3535
Documento di policy JSON 3535
Ulteriori informazioni 3536
AWSServiceRoleForAIDevOpsPolicy 3536
Utilizzo di questa politica 3536
Dettagli della policy 3536
Versione della politica 3536
Documento di policy JSON 3537
Ulteriori informazioni 3539
AWSServiceRoleForAmazonEKSNodegroup 3539
Utilizzo di questa politica 3539
Dettagli della policy 3539
Versione della politica 3540
Documento di policy JSON 3540
Ulteriori informazioni 3545
AWSServiceRoleForAmazonQDeveloper 3545
Utilizzo di questa politica 3546
Dettagli della policy 3546
Versione della politica 3546
Documento sulla politica JSON 3546
Ulteriori informazioni 3547
AWSServiceRoleForAWSTransform 3547
Utilizzo di questa politica 3547
Dettagli della policy 3547
Versione della politica 3548
Documento di policy JSON 3548
Ulteriori informazioni 3550
AWSServiceRoleForAWSTransformCustom 3550
Utilizzo di questa politica 3550
Dettagli della policy 3550
Versione della politica 3551
Documento di policy JSON 3551
Ulteriori informazioni 3552

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 3552
Utilizzo di questa politica 3552
Dettagli della policy 3552
Versione della politica 3552
Documento di policy JSON 3553
Ulteriori informazioni 3553
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 3553
Utilizzo di questa politica 3553
Dettagli della policy 3553
Versione della politica 3554
Documento di policy JSON 3554
Ulteriori informazioni 3554
AWSServiceRoleForCodeGuru-Profiler 3555
Utilizzo di questa politica 3555
Dettagli della policy 3555
Versione della politica 3555
Documento di policy JSON 3555
Ulteriori informazioni 3556
AWSServiceRoleForCodeWhispererPolicy 3556
Utilizzo di questa politica 3556
Dettagli della policy 3556
Versione della politica 3556
Documento di policy JSON 3557
Ulteriori informazioni 3559
AWSServiceRoleForEC2ScheduledInstances 3559
Utilizzo di questa politica 3559
Dettagli della policy 3560
Versione della politica 3560
Documento di policy JSON 3560
Ulteriori informazioni 3561
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 3561
Utilizzo di questa politica 3561
Dettagli della policy 3561
Versione della politica 3562
Documento di policy JSON 3562
Ulteriori informazioni 3562

AWSServiceRoleForImageBuilder 3562
Utilizzo di questa politica 3562
Dettagli della policy 3563
Versione della politica 3563
Documento di policy JSON 3563
Ulteriori informazioni 3574
AWSServiceRoleForIoTSiteWise 3574
Utilizzo di questa politica 3574
Dettagli della policy 3575
Versione della politica 3575
Documento di policy JSON 3575
Ulteriori informazioni 3576
AWSServiceRoleForLogDeliveryPolicy 3576
Utilizzo di questa politica 3577
Dettagli della policy 3577
Versione della politica 3577
Documento di policy JSON 3577
Ulteriori informazioni 3578
AWSServiceRoleForMonitronPolicy 3578
Utilizzo di questa politica 3578
Dettagli della policy 3578
Versione della politica 3579
Documento di policy JSON 3579
Ulteriori informazioni 3580
AWSServiceRoleForNeptuneGraphPolicy 3580
Utilizzo di questa politica 3581
Dettagli della policy 3581
Versione della politica 3581
Documento di policy JSON 3581
Ulteriori informazioni 3582
AWSServiceRoleForPrivateMarketplaceAdminPolicy 3583
Utilizzo di questa politica 3583
Dettagli della policy 3583
Versione della politica 3583
Documento di policy JSON 3583
Ulteriori informazioni 3585

AWSServiceRoleForProcurementInsightsPolicy 3585
Utilizzo di questa politica 3585
Dettagli della policy 3585
Versione della politica 3586
Documento di policy JSON 3586
Ulteriori informazioni 3586
AWSServiceRoleForSMS 3586
Utilizzo di questa politica 3587
Dettagli della policy 3587
Versione della politica 3587
Documento di policy JSON 3587
Ulteriori informazioni 3594
AWSServiceRoleForUserSubscriptions 3594
Utilizzo di questa politica 3594
Dettagli della policy 3594
Versione della politica 3594
Documento di policy JSON 3595
Ulteriori informazioni 3596
AWSServiceRolePolicyForBackupReports 3596
Utilizzo di questa politica 3596
Dettagli della policy 3596
Versione della politica 3597
Documento di policy JSON 3597
Ulteriori informazioni 3598
AWSServiceRolePolicyForBackupRestoreTesting 3598
Utilizzo di questa politica 3598
Dettagli della policy 3599
Versione della politica 3599
Documento di policy JSON 3599
Ulteriori informazioni 3602
AWSServiceRolePolicyForWorkspacesInstances 3602
Utilizzo di questa politica 3602
Dettagli della policy 3602
Versione della politica 3602
Documento di policy JSON 3603
Ulteriori informazioni 3604

AWSShieldDRTAccessPolicy 3605
Utilizzo di questa politica 3605
Dettagli della policy 3605
Versione della politica 3605
Documento di policy JSON 3605
Ulteriori informazioni 3606
AWSShieldServiceRolePolicy 3606
Utilizzo di questa politica 3607
Dettagli della policy 3607
Versione della politica 3607
Documento di policy JSON 3607
Ulteriori informazioni 3608
AWSSocialMessagingServiceRolePolicy 3608
Utilizzo di questa politica 3608
Dettagli della policy 3608
Versione della politica 3608
Documento di policy JSON 3608
Ulteriori informazioni 3609
AWSSSMForSAPServiceLinkedRolePolicy 3609
Utilizzo di questa politica 3609
Dettagli della policy 3609
Versione della politica 3610
Documento di policy JSON 3610
Ulteriori informazioni 3618
AWSSSMOpsInsightsServiceRolePolicy 3618
Utilizzo di questa politica 3619
Dettagli della policy 3619
Versione della politica 3619
Documento di policy JSON 3619
Ulteriori informazioni 3620
AWSSSODirectoryAdministrator 3620
Utilizzo di questa politica 3620
Dettagli della policy 3620
Versione della politica 3620
Documento di policy JSON 3621
Ulteriori informazioni 3621

AWSSSODirectoryReadOnly 3622
Utilizzo di questa politica 3622
Dettagli della policy 3622
Versione della politica 3622
Documento di policy JSON 3622
Ulteriori informazioni 3623
AWSSSOMasterAccountAdministrator 3623
Utilizzo di questa politica 3624
Dettagli della policy 3624
Versione della politica 3624
Documento di policy JSON 3624
Ulteriori informazioni 3627
AWSSSOMemberAccountAdministrator 3627
Utilizzo di questa politica 3627
Dettagli della policy 3627
Versione della politica 3628
Documento di policy JSON 3628
Ulteriori informazioni 3630
AWSSSOReadOnly 3630
Utilizzo di questa politica 3630
Dettagli della policy 3630
Versione della politica 3631
Documento di policy JSON 3631
Ulteriori informazioni 3632
AWSSSOServiceRolePolicy 3632
Utilizzo di questa politica 3633
Dettagli della policy 3633
Versione della politica 3633
Documento di policy JSON 3633
Ulteriori informazioni 3637
AWSStepFunctionsConsoleFullAccess 3637
Utilizzo di questa politica 3637
Dettagli della policy 3637
Versione della politica 3637
Documento di policy JSON 3638
Ulteriori informazioni 3638

AWSStepFunctionsFullAccess 3639
Utilizzo di questa politica 3639
Dettagli della policy 3639
Versione della politica 3639
Documento di policy JSON 3639
Ulteriori informazioni 3640
AWSStepFunctionsReadOnlyAccess 3640
Utilizzo di questa politica 3640
Dettagli della policy 3640
Versione della politica 3640
Documento di policy JSON 3641
Ulteriori informazioni 3641
AWSStorageGatewayFullAccess 3641
Utilizzo di questa politica 3642
Dettagli della policy 3642
Versione della politica 3642
Documento di policy JSON 3642
Ulteriori informazioni 3643
AWSStorageGatewayReadOnlyAccess 3643
Utilizzo di questa politica 3643
Dettagli della policy 3643
Versione della politica 3643
Documento di policy JSON 3644
Ulteriori informazioni 3644
AWSStorageGatewayServiceRolePolicy 3645
Utilizzo di questa politica 3645
Dettagli della policy 3645
Versione della politica 3645
Documento di policy JSON 3645
Ulteriori informazioni 3646
AWSSupplyChainFederationAdminAccess 3646
Utilizzo di questa politica 3646
Dettagli della policy 3646
Versione della politica 3646
Documento di policy JSON 3647
Ulteriori informazioni 3653

AWSSupportAccess 3653
Utilizzo di questa politica 3653
Dettagli della policy 3653
Versione della politica 3653
Documento di policy JSON 3654
Ulteriori informazioni 3654
AWSSupportAppFullAccess 3654
Utilizzo di questa politica 3654
Dettagli della policy 3655
Versione della politica 3655
Documento di policy JSON 3655
Ulteriori informazioni 3656
AWSSupportAppReadOnlyAccess 3656
Utilizzo di questa politica 3656
Dettagli della policy 3656
Versione della politica 3656
Documento di policy JSON 3657
Ulteriori informazioni 3657
AWSSupportPlansFullAccess 3657
Utilizzo di questa politica 3657
Dettagli della policy 3658
Versione della politica 3658
Documento di policy JSON 3658
Ulteriori informazioni 3658
AWSSupportPlansReadOnlyAccess 3659
Utilizzo di questa politica 3659
Dettagli della policy 3659
Versione della politica 3659
Documento di policy JSON 3659
Ulteriori informazioni 3660
AWSSupportPlansServiceRolePolicy 3660
Utilizzo di questa politica 3660
Dettagli della policy 3660
Versione della politica 3660
Documento sulla politica JSON 3661
Ulteriori informazioni 3661

AWSSupportServiceRolePolicy 3661
Utilizzo di questa politica 3662
Dettagli della policy 3662
Versione della politica 3662
Documento di policy JSON 3662
Ulteriori informazioni 3764
AWSSystemsManagerAccountDiscoveryServicePolicy 3764
Utilizzo di questa politica 3764
Dettagli della policy 3765
Versione della politica 3765
Documento di policy JSON 3765
Ulteriori informazioni 3766
AWSSystemsManagerChangeManagementServicePolicy 3766
Utilizzo di questa politica 3766
Dettagli della policy 3766
Versione della politica 3766
Documento di policy JSON 3766
Ulteriori informazioni 3769
AWSSystemsManagerEnableConfigRecordingExecutionPolicy 3769
Utilizzo di questa politica 3769
Dettagli della policy 3769
Versione della politica 3770
Documento di policy JSON 3770
Ulteriori informazioni 3772
AWSSystemsManagerEnableExplorerExecutionPolicy 3772
Utilizzo di questa politica 3772
Dettagli della policy 3772
Versione della politica 3772
Documento di policy JSON 3773
Ulteriori informazioni 3774
AWSSystemsManagerForSAPFullAccess 3774
Utilizzo di questa politica 3774
Dettagli della policy 3774
Versione della politica 3775
Documento di policy JSON 3775
Ulteriori informazioni 3776

AWSSystemsManagerForSAPReadOnlyAccess 3776
Utilizzo di questa politica 3776
Dettagli della policy 3776
Versione della politica 3777
Documento di policy JSON 3777
Ulteriori informazioni 3777
AWSSystemsManagerJustInTimeAccessServicePolicy 3777
Utilizzo di questa politica 3778
Dettagli della policy 3778
Versione della politica 3778
Documento di policy JSON 3778
Ulteriori informazioni 3783
AWSSystemsManagerJustInTimeAccessTokenPolicy 3784
Utilizzo di questa politica 3784
Dettagli della policy 3784
Versione della politica 3784
Documento di policy JSON 3784
Ulteriori informazioni 3787
AWSSystemsManagerJustInTimeAccessTokenSessionPolicy 3787
Utilizzo di questa politica 3787
Dettagli della policy 3788
Versione della politica 3788
Documento di policy JSON 3788
Ulteriori informazioni 3790
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy 3791
Utilizzo di questa politica 3791
Dettagli della policy 3791
Versione della politica 3791
Documento di policy JSON 3791
Ulteriori informazioni 3796
AWSSystemsManagerNotificationsServicePolicy 3796
Utilizzo di questa politica 3796
Dettagli della policy 3796
Versione della politica 3796
Documento di policy JSON 3797
Ulteriori informazioni 3798

AWSSystemsManagerOpsDataSyncServiceRolePolicy 3798
Utilizzo di questa politica 3798
Dettagli della policy 3798
Versione della politica 3798
Documento di policy JSON 3799
Ulteriori informazioni 3802
AWSThinkboxAssetServerPolicy 3802
Utilizzo di questa politica 3803
Dettagli della policy 3803
Versione della politica 3803
Documento di policy JSON 3803
Ulteriori informazioni 3804
AWSThinkboxAWSPortalAdminPolicy 3804
Utilizzo di questa politica 3804
Dettagli della policy 3804
Versione della politica 3804
Documento di policy JSON 3805
Ulteriori informazioni 3814
AWSThinkboxAWSPortalGatewayPolicy 3815
Utilizzo di questa politica 3815
Dettagli della policy 3815
Versione della politica 3815
Documento di policy JSON 3815
Ulteriori informazioni 3817
AWSThinkboxAWSPortalWorkerPolicy 3817
Utilizzo di questa politica 3817
Dettagli della policy 3818
Versione della politica 3818
Documento di policy JSON 3818
Ulteriori informazioni 3820
AWSThinkboxDeadlineResourceTrackerAccessPolicy 3820
Utilizzo di questa politica 3820
Dettagli della policy 3820
Versione della politica 3821
Documento di policy JSON 3821
Ulteriori informazioni 3824

AWSThinkboxDeadlineResourceTrackerAdminPolicy 3824
Utilizzo di questa politica 3824
Dettagli della policy 3824
Versione della politica 3824
Documento sulla politica JSON 3825
Ulteriori informazioni 3830
AWSThinkboxDeadlineSpotEventPluginAdminPolicy 3831
Utilizzo di questa politica 3831
Dettagli della policy 3831
Versione della politica 3831
Documento di policy JSON 3831
Ulteriori informazioni 3834
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 3834
Utilizzo di questa politica 3834
Dettagli della policy 3835
Versione della politica 3835
Documento di policy JSON 3835
Ulteriori informazioni 3836
AWSTransferConsoleFullAccess 3837
Utilizzo di questa politica 3837
Dettagli della policy 3837
Versione della politica 3837
Documento di policy JSON 3837
Ulteriori informazioni 3838
AWSTransferFullAccess 3838
Utilizzo di questa politica 3838
Dettagli della policy 3839
Versione della politica 3839
Documento di policy JSON 3839
Ulteriori informazioni 3840
AWSTransferLoggingAccess 3840
Utilizzo di questa politica 3840
Dettagli della policy 3840
Versione della politica 3840
Documento di policy JSON 3841
Ulteriori informazioni 3841

AWSTransferReadOnlyAccess 3841
Utilizzo di questa politica 3841
Dettagli della policy 3842
Versione della politica 3842
Documento di policy JSON 3842
Ulteriori informazioni 3842
AWSTransformApplicationDeploymentPolicy 3843
Utilizzo di questa politica 3843
Dettagli della policy 3843
Versione della politica 3843
Documento di policy JSON 3843
Ulteriori informazioni 3851
AWSTransformApplicationECSDeploymentPolicy 3852
Utilizzo di questa politica 3852
Dettagli della policy 3852
Versione della politica 3852
Documento di policy JSON 3852
Ulteriori informazioni 3860
AWSTransformCustomExecuteTransformations 3860
Utilizzo di questa politica 3861
Dettagli della policy 3861
Versione della politica 3861
Documento di policy JSON 3861
Ulteriori informazioni 3862
AWSTransformCustomFullAccess 3862
Utilizzo di questa politica 3862
Dettagli della policy 3862
Versione della politica 3863
Documento di policy JSON 3863
Ulteriori informazioni 3864
AWSTransformCustomManageTransformations 3864
Utilizzo di questa politica 3864
Dettagli della policy 3864
Versione della politica 3864
Documento di policy JSON 3865
Ulteriori informazioni 3866

AWSTransformInfrastructureExecutorAccessBatch 3866
Utilizzo di questa politica 3866
Dettagli della policy 3866
Versione della politica 3867
Documento sulla politica JSON 3867
Ulteriori informazioni 3873
AWSTransformInfrastructureExecutorAccessEC2 3873
Utilizzo di questa politica 3874
Dettagli della policy 3874
Versione della politica 3874
Documento sulla politica JSON 3874
Ulteriori informazioni 3881
AWSTransformRevenueAttributionPolicy 3881
Utilizzo di questa politica 3881
Dettagli della policy 3882
Versione della politica 3882
Documento di policy JSON 3882
Ulteriori informazioni 3883
AWSTransformSecretsManagerConnectorPolicy 3883
Utilizzo di questa politica 3883
Dettagli della policy 3883
Versione della politica 3883
Documento di policy JSON 3884
Ulteriori informazioni 3885
AWSTransformSecurityAgentExecutorAccess 3885
Utilizzo di questa politica 3885
Dettagli della policy 3885
Versione della politica 3886
Documento sulla politica JSON 3886
Ulteriori informazioni 3888
AWSTrustedAdvisorPriorityFullAccess 3888
Utilizzo di questa politica 3888
Dettagli della policy 3888
Versione della politica 3889
Documento di policy JSON 3889
Ulteriori informazioni 3890

AWSTrustedAdvisorPriorityReadOnlyAccess 3891
Utilizzo di questa politica 3891
Dettagli della policy 3891
Versione della politica 3891
Documento di policy JSON 3891
Ulteriori informazioni 3892
AWSTrustedAdvisorReportingServiceRolePolicy 3893
Utilizzo di questa politica 3893
Dettagli della policy 3893
Versione della politica 3893
Documento di policy JSON 3893
Ulteriori informazioni 3894
AWSTrustedAdvisorServiceRolePolicy 3894
Utilizzo di questa politica 3894
Dettagli della policy 3894
Versione della politica 3895
Documento di policy JSON 3895
Ulteriori informazioni 3898
AWSUserAttributeCostAllocationPolicy 3898
Utilizzo di questa politica 3898
Dettagli della policy 3898
Versione della politica 3898
Documento di policy JSON 3899
Ulteriori informazioni 3899
AWSUserNotificationsServiceLinkedRolePolicy 3899
Utilizzo di questa politica 3899
Dettagli della policy 3899
Versione della politica 3900
Documento di policy JSON 3900
Ulteriori informazioni 3902
AWSVendorInsightsAssessorFullAccess 3902
Utilizzo di questa politica 3902
Dettagli della policy 3902
Versione della politica 3902
Documento di policy JSON 3902
Ulteriori informazioni 3903

AWSVendorInsightsAssessorReadOnly 3904
Utilizzo di questa politica 3904
Dettagli della policy 3904
Versione della politica 3904
Documento di policy JSON 3904
Ulteriori informazioni 3905
AWSVendorInsightsVendorFullAccess 3905
Utilizzo di questa politica 3905
Dettagli della policy 3905
Versione della politica 3906
Documento di policy JSON 3906
Ulteriori informazioni 3907
AWSVendorInsightsVendorReadOnly 3908
Utilizzo di questa politica 3908
Dettagli della policy 3908
Versione della politica 3908
Documento di policy JSON 3908
Ulteriori informazioni 3909
AWSVPCFlowLogsServiceRolePolicy 3910
Utilizzo di questa politica 3910
Dettagli della policy 3910
Versione della politica 3910
Documento di policy JSON 3910
Ulteriori informazioni 3912
AWSVpcLatticeServiceRolePolicy 3912
Utilizzo di questa politica 3912
Dettagli della policy 3912
Versione della politica 3912
Documento di policy JSON 3913
Ulteriori informazioni 3915
AWSVPCS2SVpnServiceRolePolicy 3915
Utilizzo di questa politica 3916
Dettagli della policy 3916
Versione della politica 3916
Documento di policy JSON 3916
Ulteriori informazioni 3917

AWSVPCTransitGatewayServiceRolePolicy 3917
Utilizzo di questa politica 3918
Dettagli della policy 3918
Versione della politica 3918
Documento di policy JSON 3918
Ulteriori informazioni 3919
AWSVPCVerifiedAccessServiceRolePolicy 3919
Utilizzo di questa politica 3919
Dettagli della policy 3919
Versione della politica 3919
Documento di policy JSON 3920
Ulteriori informazioni 3921
AWSWAFConsoleFullAccess 3921
Utilizzo di questa politica 3922
Dettagli della policy 3922
Versione della politica 3922
Documento di policy JSON 3922
Ulteriori informazioni 3931
AWSWAFConsoleReadOnlyAccess 3931
Utilizzo di questa politica 3932
Dettagli della policy 3932
Versione della politica 3932
Documento di policy JSON 3932
Ulteriori informazioni 3940
AWSWAFFullAccess 3940
Utilizzo di questa politica 3940
Dettagli della policy 3940
Versione della politica 3940
Documento sulla politica JSON 3941
Ulteriori informazioni 3946
AWSWAFReadOnlyAccess 3947
Utilizzo di questa politica 3947
Dettagli della policy 3947
Versione della politica 3947
Documento di policy JSON 3947
Ulteriori informazioni 3951

AWSWellArchitectedDiscoveryServiceRolePolicy 3952
Utilizzo di questa politica 3952
Dettagli della policy 3952
Versione della politica 3952
Documento di policy JSON 3952
Ulteriori informazioni 3954
AWSWellArchitectedOrganizationsServiceRolePolicy 3954
Utilizzo di questa politica 3954
Dettagli della policy 3954
Versione della politica 3954
Documento di policy JSON 3955
Ulteriori informazioni 3955
AWSWickrFullAccess 3955
Utilizzo di questa politica 3956
Dettagli della policy 3956
Versione della politica 3956
Documento di policy JSON 3956
Ulteriori informazioni 3956
AWSXrayCrossAccountSharingConfiguration 3957
Utilizzo di questa politica 3957
Dettagli della policy 3957
Versione della politica 3957
Documento di policy JSON 3957
Ulteriori informazioni 3958
AWSXRayDaemonWriteAccess 3958
Utilizzo di questa politica 3959
Dettagli della policy 3959
Versione della politica 3959
Documento di policy JSON 3959
Ulteriori informazioni 3960
AWSXrayFullAccess 3960
Utilizzo di questa politica 3960
Dettagli della policy 3960
Versione della politica 3960
Documento di policy JSON 3960
Ulteriori informazioni 3961

AWSXrayReadOnlyAccess 3961
Utilizzo di questa politica 3961
Dettagli della policy 3961
Versione della politica 3962
Documento di policy JSON 3962
Ulteriori informazioni 3963
AWSXrayWriteOnlyAccess 3963
Utilizzo di questa politica 3963
Dettagli della policy 3963
Versione della politica 3963
Documento di policy JSON 3963
Ulteriori informazioni 3964
AWSZonalAutoshiftPracticeRunSLRPolicy 3964
Utilizzo di questa politica 3964
Dettagli della policy 3964
Versione della politica 3965
Documento di policy JSON 3965
Ulteriori informazioni 3966
AWSZoneGroupAccessManagementServiceRolePolicy 3966
Utilizzo di questa politica 3966
Dettagli della policy 3966
Versione della politica 3966
Documento di policy JSON 3967
Ulteriori informazioni 3967
BatchServiceRolePolicy 3967
Utilizzo di questa politica 3968
Dettagli della policy 3968
Versione della politica 3968
Documento di policy JSON 3968
Ulteriori informazioni 3974
BedrockAgentCoreFullAccess 3974
Utilizzo di questa politica 3974
Dettagli della policy 3975
Versione della politica 3975
Documento sulla politica JSON 3975
Ulteriori informazioni 3985

BedrockAgentCoreNetworkServiceRolePolicy 3985
Utilizzo di questa politica 3985
Dettagli della policy 3985
Versione della politica 3986
Documento di policy JSON 3986
Ulteriori informazioni 3988
BedrockAgentCoreRuntimeIdentityServiceRolePolicy 3988
Utilizzo di questa politica 3988
Dettagli della policy 3988
Versione della politica 3988
Documento di policy JSON 3989
Ulteriori informazioni 3989
Billing 3989
Utilizzo di questa politica 3989
Dettagli della policy 3989
Versione della politica 3990
Documento sulla politica JSON 3990
Ulteriori informazioni 3994
BudgetsServiceRolePolicy 3994
Utilizzo di questa politica 3994
Dettagli della policy 3994
Versione della politica 3994
Documento di policy JSON 3995
Ulteriori informazioni 3995
CertificateManagerServiceRolePolicy 3995
Utilizzo di questa politica 3995
Dettagli della policy 3995
Versione della politica 3996
Documento di policy JSON 3996
Ulteriori informazioni 3996
ClientVPNServiceConnectionsRolePolicy 3996
Utilizzo di questa politica 3997
Dettagli della policy 3997
Versione della politica 3997
Documento di policy JSON 3997
Ulteriori informazioni 3997

ClientVPNServiceRolePolicy 3998
Utilizzo di questa politica 3998
Dettagli della policy 3998
Versione della politica 3998
Documento di policy JSON 3998
Ulteriori informazioni 3999
CloudFormationStackSetsOrgAdminServiceRolePolicy 3999
Utilizzo di questa politica 3999
Dettagli della policy 4000
Versione della politica 4000
Documento di policy JSON 4000
Ulteriori informazioni 4001
CloudFormationStackSetsOrgMemberServiceRolePolicy 4001
Utilizzo di questa politica 4001
Dettagli della policy 4001
Versione della politica 4001
Documento sulla politica JSON 4001
Ulteriori informazioni 4003
CloudFrontFullAccess 4003
Utilizzo di questa politica 4003
Dettagli della policy 4003
Versione della politica 4003
Documento sulla politica JSON 4004
Ulteriori informazioni 4006
CloudFrontReadOnlyAccess 4006
Utilizzo di questa politica 4006
Dettagli della policy 4006
Versione della politica 4006
Documento di policy JSON 4007
Ulteriori informazioni 4007
CloudHSMServiceRolePolicy 4008
Utilizzo di questa politica 4008
Dettagli della policy 4008
Versione della politica 4008
Documento di policy JSON 4008
Ulteriori informazioni 4009

CloudSearchFullAccess 4009
Utilizzo di questa politica 4009
Dettagli della policy 4009
Versione della politica 4009
Documento di policy JSON 4010
Ulteriori informazioni 4010
CloudSearchReadOnlyAccess 4010
Utilizzo di questa politica 4010
Dettagli della policy 4010
Versione della politica 4011
Documento di policy JSON 4011
Ulteriori informazioni 4011
CloudTrailEventContext 4011
Utilizzo di questa politica 4012
Dettagli della policy 4012
Versione della politica 4012
Documento di policy JSON 4012
Ulteriori informazioni 4014
CloudTrailServiceRolePolicy 4014
Utilizzo di questa politica 4014
Dettagli della policy 4014
Versione della politica 4014
Documento di policy JSON 4015
Ulteriori informazioni 4016
CloudWatch-CrossAccountAccess 4016
Utilizzo di questa politica 4017
Dettagli della policy 4017
Versione della politica 4017
Documento di policy JSON 4017
Ulteriori informazioni 4018
CloudWatchActionsEC2Access 4018
Utilizzo di questa politica 4018
Dettagli della policy 4018
Versione della politica 4018
Documento di policy JSON 4018
Ulteriori informazioni 4019

CloudWatchAgentAdminPolicy 4019
Utilizzo di questa politica 4019
Dettagli della policy 4019
Versione della politica 4020
Documento di policy JSON 4020
Ulteriori informazioni 4021
CloudWatchAgentServerPolicy 4021
Utilizzo di questa politica 4021
Dettagli della policy 4021
Versione della politica 4021
Documento di policy JSON 4021
Ulteriori informazioni 4022
CloudWatchAPIKeyAccess 4023
Utilizzo di questa politica 4023
Dettagli della policy 4023
Versione della politica 4023
Documento di policy JSON 4023
Ulteriori informazioni 4024
CloudWatchApplicationInsightsFullAccess 4024
Utilizzo di questa politica 4024
Dettagli della policy 4024
Versione della politica 4025
Documento di policy JSON 4025
Ulteriori informazioni 4026
CloudWatchApplicationInsightsReadOnlyAccess 4026
Utilizzo di questa politica 4027
Dettagli della policy 4027
Versione della politica 4027
Documento di policy JSON 4027
Ulteriori informazioni 4027
CloudwatchApplicationInsightsServiceLinkedRolePolicy 4028
Utilizzo di questa politica 4028
Dettagli della policy 4028
Versione della politica 4028
Documento di policy JSON 4028
Ulteriori informazioni 4039

CloudWatchApplicationSignalsFullAccess 4039
Utilizzo di questa politica 4039
Dettagli della policy 4039
Versione della politica 4040
Documento di policy JSON 4040
Ulteriori informazioni 4045
CloudWatchApplicationSignalsReadOnlyAccess 4045
Utilizzo di questa politica 4045
Dettagli della policy 4045
Versione della politica 4046
Documento di policy JSON 4046
Ulteriori informazioni 4050
CloudWatchApplicationSignalsServiceRolePolicy 4050
Utilizzo di questa politica 4050
Dettagli della policy 4050
Versione della politica 4051
Documento di policy JSON 4051
Ulteriori informazioni 4054
CloudWatchAutomaticDashboardsAccess 4054
Utilizzo di questa politica 4054
Dettagli della policy 4054
Versione della politica 4054
Documento di policy JSON 4055
Ulteriori informazioni 4056
CloudWatchCrossAccountSharingConfiguration 4056
Utilizzo di questa politica 4056
Dettagli della policy 4056
Versione della politica 4057
Documento di policy JSON 4057
Ulteriori informazioni 4058
CloudWatchEventsBuiltInTargetExecutionAccess 4058
Utilizzo di questa politica 4058
Dettagli della policy 4058
Versione della politica 4058
Documento di policy JSON 4059
Ulteriori informazioni 4059

CloudWatchEventsFullAccess 4059
Utilizzo di questa politica 4059
Dettagli della policy 4059
Versione della politica 4060
Documento di policy JSON 4060
Ulteriori informazioni 4062
CloudWatchEventsInvocationAccess 4062
Utilizzo di questa politica 4062
Dettagli della policy 4062
Versione della politica 4063
Documento di policy JSON 4063
Ulteriori informazioni 4063
CloudWatchEventsReadOnlyAccess 4063
Utilizzo di questa politica 4063
Dettagli della policy 4064
Versione della politica 4064
Documento di policy JSON 4064
Ulteriori informazioni 4065
CloudWatchEventsServiceRolePolicy 4066
Utilizzo di questa politica 4066
Dettagli della policy 4066
Versione della politica 4066
Documento di policy JSON 4066
Ulteriori informazioni 4067
CloudWatchFullAccess 4067
Utilizzo di questa politica 4067
Dettagli della policy 4067
Versione della politica 4067
Documento di policy JSON 4068
Ulteriori informazioni 4069
CloudWatchFullAccessV2 4069
Utilizzo di questa politica 4069
Dettagli della policy 4069
Versione della politica 4069
Documento di policy JSON 4069
Ulteriori informazioni 4075

CloudWatchInternetMonitorFullAccess 4076
Utilizzo di questa politica 4076
Dettagli della policy 4076
Versione della politica 4076
Documento di policy JSON 4076
Ulteriori informazioni 4078
CloudWatchInternetMonitorReadOnlyAccess 4078
Utilizzo di questa politica 4079
Dettagli della policy 4079
Versione della politica 4079
Documento di policy JSON 4079
Ulteriori informazioni 4080
CloudWatchInternetMonitorServiceRolePolicy 4080
Utilizzo di questa politica 4080
Dettagli della policy 4080
Versione della politica 4081
Documento di policy JSON 4081
Ulteriori informazioni 4082
CloudWatchLambdaApplicationSignalsExecutionRolePolicy 4082
Utilizzo di questa politica 4082
Dettagli della policy 4082
Versione della politica 4082
Documento di policy JSON 4083
Ulteriori informazioni 4084
CloudWatchLambdaInsightsExecutionRolePolicy 4084
Utilizzo di questa politica 4084
Dettagli della policy 4084
Versione della politica 4084
Documento di policy JSON 4084
Ulteriori informazioni 4085
CloudWatchLogsAPIKeyAccess 4085
Utilizzo di questa politica 4085
Dettagli della policy 4085
Versione della politica 4086
Documento di policy JSON 4086
Ulteriori informazioni 4087

CloudWatchLogsCrossAccountSharingConfiguration 4087
Utilizzo di questa politica 4087
Dettagli della policy 4087
Versione della politica 4088
Documento di policy JSON 4088
Ulteriori informazioni 4089
CloudWatchLogsFullAccess 4089
Utilizzo di questa politica 4089
Dettagli della policy 4089
Versione della politica 4089
Documento di policy JSON 4090
Ulteriori informazioni 4090
CloudWatchLogsReadOnlyAccess 4090
Utilizzo di questa politica 4090
Dettagli della policy 4091
Versione della politica 4091
Documento di policy JSON 4091
Ulteriori informazioni 4092
CloudWatchNetworkFlowMonitorAgentPublishPolicy 4092
Utilizzo di questa politica 4092
Dettagli della policy 4092
Versione della politica 4092
Documento di policy JSON 4093
Ulteriori informazioni 4093
CloudWatchNetworkFlowMonitorServiceRolePolicy 4093
Utilizzo di questa politica 4094
Dettagli della policy 4094
Versione della politica 4094
Documento di policy JSON 4094
Ulteriori informazioni 4095
CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy 4095
Utilizzo di questa politica 4095
Dettagli della policy 4096
Versione della politica 4096
Documento di policy JSON 4096
Ulteriori informazioni 4097

CloudWatchNetworkMonitorServiceRolePolicy 4097
Utilizzo di questa politica 4097
Dettagli della policy 4097
Versione della politica 4098
Documento di policy JSON 4098
Ulteriori informazioni 4099
CloudWatchOpenSearchDashboardAccess 4099
Utilizzo di questa politica 4100
Dettagli della policy 4100
Versione della politica 4100
Documento di policy JSON 4100
Ulteriori informazioni 4102
CloudWatchOpenSearchDashboardsFullAccess 4103
Utilizzo di questa politica 4103
Dettagli della policy 4103
Versione della politica 4103
Documento di policy JSON 4103
Ulteriori informazioni 4110
CloudWatchReadOnlyAccess 4111
Utilizzo di questa politica 4111
Dettagli della policy 4111
Versione della politica 4111
Documento di policy JSON 4111
Ulteriori informazioni 4114
CloudWatchSyntheticsFullAccess 4114
Utilizzo di questa politica 4114
Dettagli della policy 4114
Versione della politica 4115
Documento di policy JSON 4115
Ulteriori informazioni 4120
CloudWatchSyntheticsReadOnlyAccess 4120
Utilizzo di questa politica 4121
Dettagli della policy 4121
Versione della politica 4121
Documento di policy JSON 4121
Ulteriori informazioni 4122

ComprehendDataAccessRolePolicy 4122
Utilizzo di questa politica 4122
Dettagli della policy 4122
Versione della politica 4122
Documento di policy JSON 4122
Ulteriori informazioni 4123
ComprehendFullAccess 4123
Utilizzo di questa politica 4123
Dettagli della policy 4123
Versione della politica 4124
Documento di policy JSON 4124
Ulteriori informazioni 4124
ComprehendMedicalFullAccess 4124
Utilizzo di questa politica 4125
Dettagli della policy 4125
Versione della politica 4125
Documento di policy JSON 4125
Ulteriori informazioni 4125
ComprehendReadOnly 4126
Utilizzo di questa politica 4126
Dettagli della policy 4126
Versione della politica 4126
Documento di policy JSON 4126
Ulteriori informazioni 4128
ComputeOptimizerAutomationServiceRolePolicy 4128
Utilizzo di questa politica 4128
Dettagli della policy 4128
Versione della politica 4128
Documento di policy JSON 4129
Ulteriori informazioni 4130
ComputeOptimizerReadOnlyAccess 4130
Utilizzo di questa politica 4131
Dettagli della policy 4131
Versione della politica 4131
Documento di policy JSON 4131
Ulteriori informazioni 4132

ComputeOptimizerServiceRolePolicy 4132
Utilizzo di questa politica 4133
Dettagli della policy 4133
Versione della politica 4133
Documento di policy JSON 4133
Ulteriori informazioni 4136
ConfigConformsServiceRolePolicy 4136
Utilizzo di questa politica 4136
Dettagli della policy 4136
Versione della politica 4136
Documento di policy JSON 4137
Ulteriori informazioni 4139
ConsoleFullAccessFromVercel 4139
Utilizzo di questa politica 4140
Dettagli della policy 4140
Versione della politica 4140
Documento di policy JSON 4140
Ulteriori informazioni 4145
ConsoleViewOnlyAccessFromVercel 4145
Utilizzo di questa politica 4145
Dettagli della policy 4145
Versione della politica 4146
Documento di policy JSON 4146
Ulteriori informazioni 4148
CostOptimizationHubAdminAccess 4149
Utilizzo di questa politica 4149
Dettagli della policy 4149
Versione della politica 4149
Documento di policy JSON 4149
Ulteriori informazioni 4150
CostOptimizationHubReadOnlyAccess 4151
Utilizzo di questa politica 4151
Dettagli della policy 4151
Versione della politica 4151
Documento di policy JSON 4151
Ulteriori informazioni 4152

CostOptimizationHubServiceRolePolicy 4152
Utilizzo di questa politica 4152
Dettagli della policy 4152
Versione della politica 4153
Documento di policy JSON 4153
Ulteriori informazioni 4154
CustomerProfilesServiceLinkedRolePolicy 4154
Utilizzo di questa politica 4154
Dettagli della policy 4154
Versione della politica 4155
Documento di policy JSON 4155
Ulteriori informazioni 4156
DatabaseAdministrator 4156
Utilizzo di questa politica 4156
Dettagli della policy 4156
Versione della politica 4156
Documento di policy JSON 4157
Ulteriori informazioni 4159
DataScientist 4160
Utilizzo di questa politica 4160
Dettagli della policy 4160
Versione della politica 4160
Documento di policy JSON 4160
Ulteriori informazioni 4164
DAXServiceRolePolicy 4164
Utilizzo di questa politica 4164
Dettagli della policy 4164
Versione della politica 4165
Documento di policy JSON 4165
Ulteriori informazioni 4165
DBModDiscoveryAndAssessment 4166
Utilizzo di questa politica 4166
Dettagli della policy 4166
Versione della politica 4166
Documento di policy JSON 4166
Ulteriori informazioni 4170

DBModProvisioningAndMigration 4170
Utilizzo di questa politica 4170
Dettagli della policy 4171
Versione della politica 4171
Documento di policy JSON 4171
Ulteriori informazioni 4176
DBModVirtualSource 4176
Utilizzo di questa politica 4176
Dettagli della policy 4176
Versione della politica 4176
Documento di policy JSON 4177
Ulteriori informazioni 4181
DeclarativePoliciesEC2Report 4181
Utilizzo di questa politica 4181
Dettagli della policy 4181
Versione della politica 4182
Documento di policy JSON 4182
Ulteriori informazioni 4182
DynamoDBCloudWatchContributorInsightsServiceRolePolicy 4183
Utilizzo di questa politica 4183
Dettagli della policy 4183
Versione della politica 4183
Documento di policy JSON 4183
Ulteriori informazioni 4184
DynamoDBGlobalTableSettingsManagementServiceRolePolicy 4184
Utilizzo di questa politica 4184
Dettagli della policy 4184
Versione della politica 4185
Documento di policy JSON 4185
Ulteriori informazioni 4186
DynamoDBKinesisReplicationServiceRolePolicy 4186
Utilizzo di questa politica 4186
Dettagli della policy 4186
Versione della politica 4186
Documento di policy JSON 4187
Ulteriori informazioni 4187

DynamoDBReplicationServiceRolePolicy 4187
Utilizzo di questa politica 4188
Dettagli della policy 4188
Versione della politica 4188
Documento di policy JSON 4188
Ulteriori informazioni 4189
EC2ApplicationStatusChecksServiceRolePolicy 4189
Utilizzo di questa politica 4190
Dettagli della policy 4190
Versione della politica 4190
Documento sulla politica JSON 4190
Ulteriori informazioni 4191
EC2FastLaunchFullAccess 4191
Utilizzo di questa politica 4191
Dettagli della policy 4192
Versione della politica 4192
Documento di policy JSON 4192
Ulteriori informazioni 4199
EC2FastLaunchServiceRolePolicy 4199
Utilizzo di questa politica 4199
Dettagli della policy 4199
Versione della politica 4200
Documento di policy JSON 4200
Ulteriori informazioni 4206
EC2FleetTimeShiftableServiceRolePolicy 4206
Utilizzo di questa politica 4206
Dettagli della policy 4206
Versione della politica 4206
Documento di policy JSON 4207
Ulteriori informazioni 4208
Ec2ImageBuilderCrossAccountDistributionAccess 4208
Utilizzo di questa politica 4208
Dettagli della policy 4208
Versione della politica 4209
Documento di policy JSON 4209
Ulteriori informazioni 4209

EC2ImageBuilderExecutionPolicy 4210
Utilizzo di questa politica 4210
Dettagli della policy 4210
Versione della politica 4210
Documento di policy JSON 4210
Ulteriori informazioni 4226
EC2ImageBuilderLifecycleExecutionPolicy 4226
Utilizzo di questa politica 4226
Dettagli della policy 4226
Versione della politica 4226
Documento di policy JSON 4227
Ulteriori informazioni 4228
EC2InstanceConnect 4229
Utilizzo di questa politica 4229
Dettagli della policy 4229
Versione della politica 4229
Documento di policy JSON 4229
Ulteriori informazioni 4230
Ec2InstanceConnectEndpoint 4230
Utilizzo di questa politica 4230
Dettagli della policy 4230
Versione della politica 4230
Documento di policy JSON 4231
Ulteriori informazioni 4233
EC2InstanceProfileForImageBuilder 4233
Utilizzo di questa politica 4234
Dettagli della policy 4234
Versione della politica 4234
Documento di policy JSON 4234
Ulteriori informazioni 4237
EC2InstanceProfileForImageBuilderECRContainerBuilds 4237
Utilizzo di questa politica 4237
Dettagli della policy 4237
Versione della politica 4237
Documento di policy JSON 4238
Ulteriori informazioni 4239

ECRReplicationServiceRolePolicy 4239
Utilizzo di questa politica 4239
Dettagli della policy 4239
Versione della politica 4240
Documento di policy JSON 4240
Ulteriori informazioni 4240
ECRTemplateServiceRolePolicy 4240
Utilizzo di questa politica 4241
Dettagli della policy 4241
Versione della politica 4241
Documento di policy JSON 4241
Ulteriori informazioni 4242
ElastiCacheServiceRolePolicy 4242
Utilizzo di questa politica 4242
Dettagli della policy 4242
Versione della politica 4242
Documento di policy JSON 4242
Ulteriori informazioni 4244
ElasticLoadBalancingFullAccess 4245
Utilizzo di questa politica 4245
Dettagli della policy 4245
Versione della politica 4245
Documento di policy JSON 4245
Ulteriori informazioni 4247
ElasticLoadBalancingReadOnly 4247
Utilizzo di questa politica 4247
Dettagli della policy 4247
Versione della politica 4247
Documento di policy JSON 4247
Ulteriori informazioni 4248
ElementalActivationsDownloadSoftwareAccess 4249
Utilizzo di questa politica 4249
Dettagli della policy 4249
Versione della politica 4249
Documento di policy JSON 4249
Ulteriori informazioni 4250

ElementalActivationsFullAccess 4250
Utilizzo di questa politica 4250
Dettagli della policy 4250
Versione della politica 4250
Documento di policy JSON 4251
Ulteriori informazioni 4251
ElementalActivationsGenerateLicenses 4251
Utilizzo di questa politica 4251
Dettagli della policy 4252
Versione della politica 4252
Documento di policy JSON 4252
Ulteriori informazioni 4252
ElementalActivationsReadOnlyAccess 4253
Utilizzo di questa politica 4253
Dettagli della policy 4253
Versione della politica 4253
Documento di policy JSON 4253
Ulteriori informazioni 4254
ElementalAppliancesSoftwareFullAccess 4254
Utilizzo di questa politica 4254
Dettagli della policy 4254
Versione della politica 4254
Documento di policy JSON 4255
Ulteriori informazioni 4255
ElementalAppliancesSoftwareReadOnlyAccess 4255
Utilizzo di questa politica 4255
Dettagli della policy 4256
Versione della politica 4256
Documento di policy JSON 4256
Ulteriori informazioni 4256
ElementalSupportCenterFullAccess 4257
Utilizzo di questa politica 4257
Dettagli della policy 4257
Versione della politica 4257
Documento di policy JSON 4257
Ulteriori informazioni 4258

EMRDescribeClusterPolicyForEMRWAL 4258
Utilizzo di questa politica 4258
Dettagli della policy 4258
Versione della politica 4258
Documento di policy JSON 4259
Ulteriori informazioni 4259
FinOpsAgentAgentPolicy 4259
Utilizzo di questa politica 4259
Dettagli della policy 4259
Versione della politica 4260
Documento di policy JSON 4260
Ulteriori informazioni 4263
FinOpsAgentOperatorPolicy 4263
Utilizzo di questa politica 4263
Dettagli della policy 4263
Versione della politica 4263
Documento di policy JSON 4263
Ulteriori informazioni 4264
FMSServiceRolePolicy 4265
Utilizzo di questa politica 4265
Dettagli della policy 4265
Versione della politica 4265
Documento di policy JSON 4265
Ulteriori informazioni 4282
FSxDeleteServiceLinkedRoleAccess 4282
Utilizzo di questa politica 4282
Dettagli della policy 4282
Versione della politica 4283
Documento di policy JSON 4283
Ulteriori informazioni 4283
GameLiftContainerFleetPolicy 4283
Utilizzo di questa politica 4284
Dettagli della policy 4284
Versione della politica 4284
Documento di policy JSON 4284
Ulteriori informazioni 4285

GameLiftGameServerGroupPolicy 4285
Utilizzo di questa politica 4286
Dettagli della policy 4286
Versione della politica 4286
Documento di policy JSON 4286
Ulteriori informazioni 4288
GitLabDuoWithAmazonQPermissionsPolicy 4288
Utilizzo di questa politica 4288
Dettagli della policy 4288
Versione della politica 4288
Documento di policy JSON 4289
Ulteriori informazioni 4290
GlobalAcceleratorFullAccess 4290
Utilizzo di questa politica 4290
Dettagli della policy 4290
Versione della politica 4290
Documento di policy JSON 4290
Ulteriori informazioni 4291
GlobalAcceleratorReadOnlyAccess 4292
Utilizzo di questa politica 4292
Dettagli della policy 4292
Versione della politica 4292
Documento di policy JSON 4292
Ulteriori informazioni 4293
GreengrassOTAUpdateArtifactAccess 4293
Utilizzo di questa politica 4293
Dettagli della policy 4293
Versione della politica 4293
Documento di policy JSON 4293
Ulteriori informazioni 4294
GroundTruthSyntheticConsoleFullAccess 4294
Utilizzo di questa politica 4294
Dettagli della policy 4294
Versione della politica 4295
Documento di policy JSON 4295
Ulteriori informazioni 4295

GroundTruthSyntheticConsoleReadOnlyAccess 4295
Utilizzo di questa politica 4296
Dettagli della policy 4296
Versione della politica 4296
Documento di policy JSON 4296
Ulteriori informazioni 4297
Health_OrganizationsServiceRolePolicy 4297
Utilizzo di questa politica 4297
Dettagli della policy 4297
Versione della politica 4297
Documento di policy JSON 4297
Ulteriori informazioni 4298
IAMAccessAdvisorReadOnly 4298
Utilizzo di questa politica 4298
Dettagli della policy 4298
Versione della politica 4299
Documento di policy JSON 4299
Ulteriori informazioni 4300
IAMAccessAnalyzerFullAccess 4300
Utilizzo di questa politica 4300
Dettagli della policy 4300
Versione della politica 4300
Documento di policy JSON 4300
Ulteriori informazioni 4301
IAMAccessAnalyzerReadOnlyAccess 4302
Utilizzo di questa politica 4302
Dettagli della policy 4302
Versione della politica 4302
Documento di policy JSON 4302
Ulteriori informazioni 4303
IAMFullAccess 4303
Utilizzo di questa politica 4303
Dettagli della policy 4303
Versione della politica 4303
Documento di policy JSON 4304
Ulteriori informazioni 4304

IAMReadOnlyAccess 4304
Utilizzo di questa politica 4305
Dettagli della policy 4305
Versione della politica 4305
Documento di policy JSON 4305
Ulteriori informazioni 4306
IAMSelfManageServiceSpecificCredentials 4306
Utilizzo di questa politica 4306
Dettagli della policy 4306
Versione della politica 4306
Documento di policy JSON 4306
Ulteriori informazioni 4307
IAMUserChangePassword 4307
Utilizzo di questa politica 4307
Dettagli della policy 4307
Versione della politica 4308
Documento di policy JSON 4308
Ulteriori informazioni 4308
IAMUserSSHKeys 4309
Utilizzo di questa politica 4309
Dettagli della policy 4309
Versione della politica 4309
Documento di policy JSON 4309
Ulteriori informazioni 4310
IVSFullAccess 4310
Utilizzo di questa politica 4310
Dettagli della policy 4310
Versione della politica 4310
Documento di policy JSON 4311
Ulteriori informazioni 4311
IVSReadOnlyAccess 4311
Utilizzo di questa politica 4311
Dettagli della policy 4312
Versione della politica 4312
Documento di policy JSON 4312
Ulteriori informazioni 4313

IVSRecordToS3 4313
Utilizzo di questa politica 4314
Dettagli della policy 4314
Versione della politica 4314
Documento di policy JSON 4314
Ulteriori informazioni 4315
KafkaConnectServiceRolePolicy 4315
Utilizzo di questa politica 4315
Dettagli della policy 4315
Versione della politica 4315
Documento di policy JSON 4315
Ulteriori informazioni 4317
KafkaServiceRolePolicy 4317
Utilizzo di questa politica 4317
Dettagli della policy 4317
Versione della politica 4317
Documento di policy JSON 4318
Ulteriori informazioni 4319
KeyspacesCDCServiceRolePolicy 4320
Utilizzo di questa politica 4320
Dettagli della policy 4320
Versione della politica 4320
Documento di policy JSON 4320
Ulteriori informazioni 4321
KeyspacesReplicationServiceRolePolicy 4321
Utilizzo di questa politica 4321
Dettagli della policy 4321
Versione della politica 4321
Documento di policy JSON 4322
Ulteriori informazioni 4323
LakeFormationDataAccessServiceRolePolicy 4323
Utilizzo di questa politica 4323
Dettagli della policy 4323
Versione della politica 4324
Documento di policy JSON 4324
Ulteriori informazioni 4324

LexBotPolicy 4324
Utilizzo di questa politica 4325
Dettagli della policy 4325
Versione della politica 4325
Documento di policy JSON 4325
Ulteriori informazioni 4326
LexChannelPolicy 4326
Utilizzo di questa politica 4326
Dettagli della policy 4326
Versione della politica 4326
Documento di policy JSON 4327
Ulteriori informazioni 4327
LightsailExportAccess 4327
Utilizzo di questa politica 4327
Dettagli della policy 4327
Versione della politica 4328
Documento di policy JSON 4328
Ulteriori informazioni 4329
MediaConnectGatewayInstanceRolePolicy 4329
Utilizzo di questa politica 4329
Dettagli della policy 4329
Versione della politica 4329
Documento di policy JSON 4329
Ulteriori informazioni 4330
MediaPackageServiceRolePolicy 4330
Utilizzo di questa politica 4330
Dettagli della policy 4330
Versione della politica 4331
Documento di policy JSON 4331
Ulteriori informazioni 4331
MemoryDBServiceRolePolicy 4331
Utilizzo di questa politica 4332
Dettagli della policy 4332
Versione della politica 4332
Documento di policy JSON 4332
Ulteriori informazioni 4334

MigrationHubDMSAccessServiceRolePolicy 4334
Utilizzo di questa politica 4335
Dettagli della policy 4335
Versione della politica 4335
Documento di policy JSON 4335
Ulteriori informazioni 4336
MigrationHubServiceRolePolicy 4336
Utilizzo di questa politica 4336
Dettagli della policy 4337
Versione della politica 4337
Documento di policy JSON 4337
Ulteriori informazioni 4338
MigrationHubSMSAccessServiceRolePolicy 4338
Utilizzo di questa politica 4339
Dettagli della policy 4339
Versione della politica 4339
Documento di policy JSON 4339
Ulteriori informazioni 4340
MonitronServiceRolePolicy 4340
Utilizzo di questa politica 4340
Dettagli della policy 4340
Versione della politica 4341
Documento di policy JSON 4341
Ulteriori informazioni 4341
MultiPartyApprovalFullAccess 4342
Utilizzo di questa politica 4342
Dettagli della policy 4342
Versione della politica 4342
Documento di policy JSON 4342
Ulteriori informazioni 4345
MultiPartyApprovalReadOnlyAccess 4345
Utilizzo di questa politica 4345
Dettagli della policy 4345
Versione della politica 4345
Documento di policy JSON 4345
Ulteriori informazioni 4347

NeptuneConsoleFullAccess 4347
Utilizzo di questa politica 4348
Dettagli della policy 4348
Versione della politica 4348
Documento di policy JSON 4348
Ulteriori informazioni 4354
NeptuneFullAccess 4354
Utilizzo di questa politica 4354
Dettagli della policy 4354
Versione della politica 4354
Documento di policy JSON 4355
Ulteriori informazioni 4358
NeptuneGraphReadOnlyAccess 4359
Utilizzo di questa politica 4359
Dettagli della policy 4359
Versione della politica 4359
Documento di policy JSON 4359
Ulteriori informazioni 4361
NeptuneReadOnlyAccess 4361
Utilizzo di questa politica 4361
Dettagli della policy 4361
Versione della politica 4361
Documento di policy JSON 4362
Ulteriori informazioni 4364
NetworkAdministrator 4364
Utilizzo di questa politica 4364
Dettagli della policy 4364
Versione della politica 4365
Documento di policy JSON 4365
Ulteriori informazioni 4372
NetworkSecurityDirectorServiceLinkedRolePolicy 4372
Utilizzo di questa politica 4372
Dettagli della policy 4372
Versione della politica 4373
Documento di policy JSON 4373
Ulteriori informazioni 4378

NovaActServiceRolePolicy 4378
Utilizzo di questa politica 4378
Dettagli della policy 4378
Versione della politica 4379
Documento di policy JSON 4379
Ulteriori informazioni 4379
OAMFullAccess 4380
Utilizzo di questa politica 4380
Dettagli della policy 4380
Versione della politica 4380
Documento di policy JSON 4380
Ulteriori informazioni 4381
OAMReadOnlyAccess 4381
Utilizzo di questa politica 4381
Dettagli della policy 4381
Versione della politica 4381
Documento di policy JSON 4381
Ulteriori informazioni 4382
OpensearchIngestionSelfManagedVpcePolicy 4382
Utilizzo di questa politica 4382
Dettagli della policy 4382
Versione della politica 4383
Documento di policy JSON 4383
Ulteriori informazioni 4383
PartnerCentralAccountManagementUserRoleAssociation 4384
Utilizzo di questa politica 4384
Dettagli della policy 4384
Versione della politica 4384
Documento di policy JSON 4384
Ulteriori informazioni 4385
PartnerCentralIncentiveBenefitManagement 4385
Utilizzo di questa politica 4385
Dettagli della policy 4385
Versione della politica 4386
Documento di policy JSON 4386
Ulteriori informazioni 4390

PowerUserAccess 4390
Utilizzo di questa politica 4390
Dettagli della policy 4390
Versione della politica 4390
Documento di policy JSON 4390
Ulteriori informazioni 4391
PricingPlanManagerFullAccess 4391
Utilizzo di questa politica 4392
Dettagli della policy 4392
Versione della politica 4392
Documento sulla politica JSON 4392
Ulteriori informazioni 4393
PricingPlanManagerReadonlyAccess 4393
Utilizzo di questa politica 4393
Dettagli della policy 4393
Versione della politica 4393
Documento sulla politica JSON 4394
Ulteriori informazioni 4394
QAppsServiceRolePolicy 4394
Utilizzo di questa politica 4394
Dettagli della policy 4394
Versione della politica 4395
Documento di policy JSON 4395
Ulteriori informazioni 4395
QBusinessQuicksightPluginPolicy 4396
Utilizzo di questa politica 4396
Dettagli della policy 4396
Versione della politica 4396
Documento di policy JSON 4396
Ulteriori informazioni 4397
QBusinessServiceRolePolicy 4397
Utilizzo di questa politica 4397
Dettagli della policy 4397
Versione della politica 4397
Documento di policy JSON 4398
Ulteriori informazioni 4399

QuickSightAccessForS3StorageManagementAnalyticsReadOnly 4399
Utilizzo di questa politica 4399
Dettagli della policy 4400
Versione della politica 4400
Documento di policy JSON 4400
Ulteriori informazioni 4401
RDSCloudHsmAuthorizationRole 4401
Utilizzo di questa politica 4401
Dettagli della policy 4401
Versione della politica 4401
Documento di policy JSON 4401
Ulteriori informazioni 4402
ReadOnlyAccess 4402
Utilizzo di questa politica 4402
Dettagli della policy 4402
Versione della politica 4403
Documento sulla politica JSON 4403
Ulteriori informazioni 4470
ReInventTicketApprovalAccess 4470
Utilizzo di questa politica 4470
Dettagli della policy 4470
Versione della politica 4471
Documento di policy JSON 4471
Ulteriori informazioni 4471
ResourceGroupsandTagEditorFullAccess 4471
Utilizzo di questa politica 4472
Dettagli della policy 4472
Versione della politica 4472
Documento di policy JSON 4472
Ulteriori informazioni 4473
ResourceGroupsandTagEditorReadOnlyAccess 4473
Utilizzo di questa politica 4473
Dettagli della policy 4473
Versione della politica 4473
Documento di policy JSON 4474
Ulteriori informazioni 4474

ResourceGroupsServiceRolePolicy 4474
Utilizzo di questa politica 4475
Dettagli della policy 4475
Versione della politica 4475
Documento di policy JSON 4475
Ulteriori informazioni 4476
ResourceGroupsTaggingAPITagUntagSupportedResources 4476
Utilizzo di questa politica 4476
Dettagli della policy 4476
Versione della politica 4476
Documento di policy JSON 4477
Ulteriori informazioni 4485
ROSAAmazonEBSCSIDriverOperatorPolicy 4485
Utilizzo di questa politica 4485
Dettagli della policy 4485
Versione della politica 4486
Documento di policy JSON 4486
Ulteriori informazioni 4489
ROSACloudNetworkConfigOperatorPolicy 4489
Utilizzo di questa politica 4489
Dettagli della policy 4489
Versione della politica 4490
Documento di policy JSON 4490
Ulteriori informazioni 4491
ROSAControlPlaneOperatorPolicy 4491
Utilizzo di questa politica 4491
Dettagli della policy 4491
Versione della politica 4491
Documento sulla politica JSON 4492
Ulteriori informazioni 4497
ROSAImageRegistryOperatorPolicy 4497
Utilizzo di questa politica 4497
Dettagli della policy 4497
Versione della politica 4497
Documento di policy JSON 4498
Ulteriori informazioni 4499

ROSAIngressOperatorPolicy 4499
Utilizzo di questa politica 4499
Dettagli della policy 4499
Versione della politica 4500
Documento di policy JSON 4500
Ulteriori informazioni 4501
ROSAInstallerPolicy 4501
Utilizzo di questa politica 4501
Dettagli della policy 4501
Versione della politica 4501
Documento di policy JSON 4502
Ulteriori informazioni 4510
ROSAKarpenterControllerPolicy 4510
Utilizzo di questa politica 4510
Dettagli della policy 4510
Versione della politica 4511
Documento sulla politica JSON 4511
Ulteriori informazioni 4517
ROSAKMSProviderPolicy 4517
Utilizzo di questa politica 4518
Dettagli della policy 4518
Versione della politica 4518
Documento di policy JSON 4518
Ulteriori informazioni 4519
ROSAKubeControllerPolicy 4519
Utilizzo di questa politica 4519
Dettagli della policy 4519
Versione della politica 4519
Documento di policy JSON 4520
Ulteriori informazioni 4524
ROSAManageSubscription 4525
Utilizzo di questa politica 4525
Dettagli della policy 4525
Versione della politica 4525
Documento di policy JSON 4525
Ulteriori informazioni 4526

ROSANodePoolManagementPolicy 4526
Utilizzo di questa politica 4526
Dettagli della policy 4526
Versione della politica 4527
Documento sulla politica JSON 4527
Ulteriori informazioni 4533
ROSASharedVPCEndpointPolicy 4534
Utilizzo di questa politica 4534
Dettagli della policy 4534
Versione della politica 4534
Documento di policy JSON 4534
Ulteriori informazioni 4538
ROSASharedVPCRoute53Policy 4538
Utilizzo di questa politica 4538
Dettagli della policy 4538
Versione della politica 4539
Documento di policy JSON 4539
Ulteriori informazioni 4540
ROSASRESupportPolicy 4540
Utilizzo di questa politica 4540
Dettagli della policy 4540
Versione della politica 4541
Documento di policy JSON 4541
Ulteriori informazioni 4546
ROSAWorkerInstancePolicy 4546
Utilizzo di questa politica 4546
Dettagli della policy 4546
Versione della politica 4546
Documento di policy JSON 4547
Ulteriori informazioni 4548
Route53RecoveryReadinessServiceRolePolicy 4548
Utilizzo di questa politica 4548
Dettagli della policy 4548
Versione della politica 4548
Documento di policy JSON 4549
Ulteriori informazioni 4552

Route53ResolverServiceRolePolicy 4552
Utilizzo di questa politica 4552
Dettagli della policy 4552
Versione della politica 4553
Documento di policy JSON 4553
Ulteriori informazioni 4553
RTBFabricServiceRolePolicy 4554
Utilizzo di questa politica 4554
Dettagli della policy 4554
Versione della politica 4554
Documento di policy JSON 4554
Ulteriori informazioni 4556
S3StorageLensServiceRolePolicy 4557
Utilizzo di questa politica 4557
Dettagli della policy 4557
Versione della politica 4557
Documento di policy JSON 4557
Ulteriori informazioni 4558
SageMakerStudioAdminIAMConsolePolicy 4558
Utilizzo di questa politica 4558
Dettagli della policy 4558
Versione della politica 4558
Documento di policy JSON 4559
Ulteriori informazioni 4570
SageMakerStudioAdminIAMDefaultExecutionPolicy 4571
Utilizzo di questa politica 4571
Dettagli della policy 4571
Versione della politica 4571
Documento sulla politica JSON 4571
Ulteriori informazioni 4597
SageMakerStudioAdminIAMPermissiveExecutionPolicy 4597
Utilizzo di questa politica 4597
Dettagli della policy 4597
Versione della politica 4597
Documento sulla politica JSON 4598
Ulteriori informazioni 4616

SageMakerStudioAdminProjectUserRolePolicy 4617
Utilizzo di questa politica 4617
Dettagli della policy 4617
Versione della politica 4617
Documento di policy JSON 4617
Ulteriori informazioni 4620
SageMakerStudioBedrockAgentServiceRolePolicy 4620
Utilizzo di questa politica 4620
Dettagli della policy 4620
Versione della politica 4620
Documento di policy JSON 4621
Ulteriori informazioni 4624
SageMakerStudioBedrockChatAgentUserRolePolicy 4624
Utilizzo di questa politica 4624
Dettagli della policy 4624
Versione della politica 4625
Documento di policy JSON 4625
Ulteriori informazioni 4629
SageMakerStudioBedrockEvaluationJobServiceRolePolicy 4629
Utilizzo di questa politica 4629
Dettagli della policy 4630
Versione della politica 4630
Documento di policy JSON 4630
Ulteriori informazioni 4633
SageMakerStudioBedrockFlowServiceRolePolicy 4634
Utilizzo di questa politica 4634
Dettagli della policy 4634
Versione della politica 4634
Documento di policy JSON 4634
Ulteriori informazioni 4638
SageMakerStudioBedrockFunctionExecutionRolePolicy 4638
Utilizzo di questa politica 4639
Dettagli della policy 4639
Versione della politica 4639
Documento di policy JSON 4639
Ulteriori informazioni 4640

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy 4640
Utilizzo di questa politica 4640
Dettagli della policy 4641
Versione della politica 4641
Documento di policy JSON 4641
Ulteriori informazioni 4642
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy 4642
Utilizzo di questa politica 4642
Dettagli della policy 4642
Versione della politica 4643
Documento di policy JSON 4643
Ulteriori informazioni 4648
SageMakerStudioBedrockPromptUserRolePolicy 4649
Utilizzo di questa politica 4649
Dettagli della policy 4649
Versione della politica 4649
Documento di policy JSON 4649
Ulteriori informazioni 4652
SageMakerStudioDomainExecutionRolePolicy 4652
Utilizzo di questa politica 4652
Dettagli della policy 4652
Versione della politica 4652
Documento sulla politica JSON 4653
Ulteriori informazioni 4659
SageMakerStudioDomainServiceRolePolicy 4659
Utilizzo di questa politica 4659
Dettagli della policy 4659
Versione della politica 4660
Documento di policy JSON 4660
Ulteriori informazioni 4661
SageMakerStudioEMRContainersSystemNamespaceRolePolicy 4661
Utilizzo di questa politica 4661
Dettagli della policy 4661
Versione della politica 4661
Documento di policy JSON 4662
Ulteriori informazioni 4663

SageMakerStudioEMRInstanceRolePolicy 4664
Utilizzo di questa politica 4664
Dettagli della policy 4664
Versione della politica 4664
Documento di policy JSON 4664
Ulteriori informazioni 4668
SageMakerStudioEMRServiceRolePolicy 4668
Utilizzo di questa politica 4668
Dettagli della policy 4668
Versione della politica 4668
Documento di policy JSON 4669
Ulteriori informazioni 4671
SageMakerStudioFullAccess 4671
Utilizzo di questa politica 4671
Dettagli della policy 4671
Versione della politica 4672
Documento di policy JSON 4672
Ulteriori informazioni 4682
SageMakerStudioProjectProvisioningRolePolicy 4682
Utilizzo di questa politica 4682
Dettagli della policy 4682
Versione della politica 4683
Documento di policy JSON 4683
Ulteriori informazioni 4752
SageMakerStudioProjectRoleMachineLearningPolicy 4752
Utilizzo di questa politica 4752
Dettagli della policy 4752
Versione della politica 4752
Documento di policy JSON 4753
Ulteriori informazioni 4783
SageMakerStudioProjectUserRolePermissionsBoundary 4783
Utilizzo di questa politica 4783
Dettagli della policy 4783
Versione della politica 4784
Documento di policy JSON 4784
Ulteriori informazioni 4839

SageMakerStudioProjectUserRolePolicy 4839
Utilizzo di questa politica 4840
Dettagli della policy 4840
Versione della politica 4840
Documento sulla politica JSON 4840
Ulteriori informazioni 4906
SageMakerStudioQueryExecutionRolePolicy 4906
Utilizzo di questa politica 4906
Dettagli della policy 4906
Versione della politica 4907
Documento di policy JSON 4907
Ulteriori informazioni 4908
SageMakerStudioUserIAMConsolePolicy 4909
Utilizzo di questa politica 4909
Dettagli della policy 4909
Versione della politica 4909
Documento di policy JSON 4909
Ulteriori informazioni 4911
SageMakerStudioUserIAMDefaultExecutionPolicy 4911
Utilizzo di questa politica 4911
Dettagli della policy 4911
Versione della politica 4912
Documento sulla politica JSON 4912
Ulteriori informazioni 4936
SageMakerStudioUserIAMPermissiveExecutionPolicy 4937
Utilizzo di questa politica 4937
Dettagli della policy 4937
Versione della politica 4937
Documento sulla politica JSON 4937
Ulteriori informazioni 4952
SecretsManagerReadWrite 4952
Utilizzo di questa politica 4952
Dettagli della policy 4952
Versione della politica 4953
Documento di policy JSON 4953
Ulteriori informazioni 4954

SecurityAgentWebAppAPIPolicy 4955
Utilizzo di questa politica 4955
Dettagli della policy 4955
Versione della politica 4955
Documento di policy JSON 4955
Ulteriori informazioni 4957
SecurityAgentWebAppPolicy 4957
Utilizzo di questa politica 4957
Dettagli della policy 4957
Versione della politica 4958
Documento sulla politica JSON 4958
Ulteriori informazioni 4959
SecurityAudit 4960
Utilizzo di questa politica 4960
Dettagli della policy 4960
Versione della politica 4960
Documento sulla politica JSON 4960
Ulteriori informazioni 4984
SecurityLakeResourceManagementServiceRolePolicy 4984
Utilizzo di questa politica 4985
Dettagli della policy 4985
Versione della politica 4985
Documento di policy JSON 4985
Ulteriori informazioni 4991
SecurityLakeServiceLinkedRole 4991
Utilizzo di questa politica 4991
Dettagli della policy 4991
Versione della politica 4991
Documento sulla politica JSON 4991
Ulteriori informazioni 4995
ServerMigration_ServiceRole 4995
Utilizzo di questa politica 4995
Dettagli della policy 4995
Versione della politica 4995
Documento di policy JSON 4995
Ulteriori informazioni 5000

ServerMigrationConnector 5000
Utilizzo di questa politica 5001
Dettagli della policy 5001
Versione della politica 5001
Documento di policy JSON 5001
Ulteriori informazioni 5003
ServerMigrationServiceConsoleFullAccess 5003
Utilizzo di questa politica 5003
Dettagli della policy 5003
Versione della politica 5003
Documento di policy JSON 5003
Ulteriori informazioni 5005
ServerMigrationServiceLaunchRole 5005
Utilizzo di questa politica 5005
Dettagli della policy 5006
Versione della politica 5006
Documento di policy JSON 5006
Ulteriori informazioni 5009
ServerMigrationServiceRoleForInstanceValidation 5009
Utilizzo di questa politica 5009
Dettagli della policy 5009
Versione della politica 5009
Documento di policy JSON 5010
Ulteriori informazioni 5010
ServiceQuotasFullAccess 5010
Utilizzo di questa politica 5010
Dettagli della policy 5011
Versione della politica 5011
Documento di policy JSON 5011
Ulteriori informazioni 5013
ServiceQuotasReadOnlyAccess 5013
Utilizzo di questa politica 5013
Dettagli della policy 5013
Versione della politica 5013
Documento di policy JSON 5013
Ulteriori informazioni 5015

ServiceQuotasServiceRolePolicy 5015
Utilizzo di questa politica 5015
Dettagli della policy 5015
Versione della politica 5016
Documento di policy JSON 5016
Ulteriori informazioni 5016
SignInLocalDevelopmentAccess 5016
Utilizzo di questa politica 5016
Dettagli della policy 5017
Versione della politica 5017
Documento di policy JSON 5017
Ulteriori informazioni 5017
SimpleWorkflowFullAccess 5018
Utilizzo di questa politica 5018
Dettagli della policy 5018
Versione della politica 5018
Documento di policy JSON 5018
Ulteriori informazioni 5019
SMSVoiceServiceRolePolicy 5019
Utilizzo di questa politica 5019
Dettagli della policy 5019
Versione della politica 5019
Documento di policy JSON 5019
Ulteriori informazioni 5020
SplitCostAllocationDataServiceRolePolicy 5020
Utilizzo di questa politica 5020
Dettagli della policy 5020
Versione della politica 5021
Documento di policy JSON 5021
Ulteriori informazioni 5021
SSMQuickSetupRolePolicy 5022
Utilizzo di questa politica 5022
Dettagli della policy 5022
Versione della politica 5022
Documento di policy JSON 5022
Ulteriori informazioni 5025

SupportUser 5025
Utilizzo di questa politica 5025
Dettagli della policy 5026
Versione della politica 5026
Documento di policy JSON 5026
Ulteriori informazioni 5031
SystemAdministrator 5031
Utilizzo di questa politica 5031
Dettagli della policy 5032
Versione della politica 5032
Documento di policy JSON 5032
Ulteriori informazioni 5038
TranslateFullAccess 5038
Utilizzo di questa politica 5039
Dettagli della policy 5039
Versione della politica 5039
Documento di policy JSON 5039
Ulteriori informazioni 5040
TranslateReadOnly 5040
Utilizzo di questa politica 5040
Dettagli della policy 5040
Versione della politica 5040
Documento di policy JSON 5040
Ulteriori informazioni 5041
ViewOnlyAccess 5041
Utilizzo di questa politica 5041
Dettagli della policy 5042
Versione della politica 5042
Documento di policy JSON 5042
Ulteriori informazioni 5052
VMImportExportRoleForAWSConnector 5052
Utilizzo di questa politica 5052
Dettagli della policy 5053
Versione della politica 5053
Documento di policy JSON 5053
Ulteriori informazioni 5054

VPCLatticeFullAccess 5054
Utilizzo di questa politica 5054
Dettagli della policy 5054
Versione della politica 5054
Documento di policy JSON 5055
Ulteriori informazioni 5057
VPCLatticeReadOnlyAccess 5057
Utilizzo di questa politica 5057
Dettagli della policy 5057
Versione della politica 5057
Documento di policy JSON 5057
Ulteriori informazioni 5058
VPCLatticeServicesInvokeAccess 5059
Utilizzo di questa politica 5059
Dettagli della policy 5059
Versione della politica 5059
Documento di policy JSON 5059
Ulteriori informazioni 5060
WAFLoggingServiceRolePolicy 5060
Utilizzo di questa politica 5060
Dettagli della policy 5060
Versione della politica 5060
Documento di policy JSON 5060
Ulteriori informazioni 5061
WAFRegionalLoggingServiceRolePolicy 5061
Utilizzo di questa politica 5062
Dettagli della policy 5062
Versione della politica 5062
Documento di policy JSON 5062
Ulteriori informazioni 5063
WAFV2LoggingServiceRolePolicy 5063
Utilizzo di questa politica 5063
Dettagli della policy 5063
Versione della politica 5064
Documento di policy JSON 5064
Ulteriori informazioni 5065

WellArchitectedAgentResourceScanning 5065
Utilizzo di questa politica 5065
Dettagli della policy 5065
Versione della politica 5065
Documento sulla politica JSON 5066
Ulteriori informazioni 5092
WellArchitectedConsoleFullAccess 5092
Utilizzo di questa politica 5092
Dettagli della policy 5092
Versione della politica 5092
Documento di policy JSON 5092
Ulteriori informazioni 5095
WellArchitectedConsoleReadOnlyAccess 5095
Utilizzo di questa politica 5095
Dettagli della policy 5095
Versione della politica 5096
Documento di policy JSON 5096
Ulteriori informazioni 5097
WorkLinkServiceRolePolicy 5097
Utilizzo di questa politica 5097
Dettagli della policy 5097
Versione della politica 5097
Documento di policy JSON 5097
Ulteriori informazioni 5098
..... 5099

Cosa sono le policy AWS gestite?

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni. Ti consentono di iniziare ad assegnare le autorizzazioni a utenti, gruppi e ruoli più facilmente che se dovessi scrivere le politiche da solo.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per l'uso da parte di tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando viene lanciato un nuovo AWS servizio o quando nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consulta la pagina Policy gestite da AWS nella Guida per l'utente di IAM.

Comprendere le pagine di riferimento delle politiche

Ogni pagina di riferimento sulle politiche include le seguenti informazioni:

- Utilizzo di questa politica: se è possibile allegare la politica a utenti, gruppi e ruoli
- Dettagli della politica
  - Tipo: il tipo di politica AWS gestita
    - `AWS managed policy`— Una politica AWS gestita standard
    - `Job function policy`— Politica in linea con le funzioni lavorative comuni del settore
    - `Service-linked role policy`— Policy associata a un ruolo collegato al servizio che consente a un servizio di eseguire azioni per conto dell'utente, ad esempio the section called "AmazonRDSPreviewServiceRolePolicy"
    - `Service role policy`— Politica progettata per funzionare con ruoli di servizio, come the section called "AWSControlTowerServiceRolePolicy"
  - Ora di creazione: quando la politica è stata creata per la prima volta
  - Ora di modifica: quando è stata modificata questa versione della politica

  - ARN: il nome Amazon Resource della policy
- Versione della policy: la versione delle autorizzazioni concesse dalla policy
- Documento sulla politica JSON: la politica JSON
- Ulteriori informazioni: collegamenti alla documentazione relativa alle AWS politiche gestite

Policy gestite obsolete AWS

AWS aggiorna AWS regolarmente le politiche gestite. Nella maggior parte dei casi, aggiungiamo autorizzazioni a una politica. Questo accade quando lanciamo un nuovo servizio o una nuova funzionalità. Per migliorare la sicurezza delle politiche AWS gestite, a volte riduciamo l'ambito delle politiche. Quando rimuoviamo le autorizzazioni da una policy, impostiamo la policy su uno stato obsoleto e ne rendiamo disponibile una nuova. Quando un servizio o una funzionalità sono AWS obsoleti, deprechiamo anche la policy gestita per quella funzionalità. AWS

Se ricevi una notifica via e-mail che indica che una politica che stai utilizzando è obsoleta, ti consigliamo di agire immediatamente. Identifica la modifica alla politica e aggiorna i flussi di lavoro. Se AWS fornisce una politica sostitutiva, pianifica di allegarla a tutte le identità interessate (utenti, gruppi e ruoli) e quindi scollegare la politica obsoleta da tali identità.

Una policy obsoleta presenta le seguenti caratteristiche:

- È stata rimossa da questa guida.
- Le autorizzazioni continuano a funzionare per tutte le identità attualmente associate.
- Negli account in cui la policy è associata a un'identità, viene visualizzata nell'elenco Policies della console IAM con un'icona di avviso accanto ad essa.
- Non può essere associata a nessuna nuova identità. Se lo si scollega da un'identità corrente, non è possibile ricollegarlo.
- Dopo averlo scollegato da tutte le entità correnti, non è più visibile.

AWS policy gestite

AWS politiche gestite

- AccessAnalyzerServiceRolePolicy
- AccountAccessManagerServiceRolePolicy
- AccountManagementFromVercel
- AdministratorAccess
- AdministratorAccess-Amplify
- AdministratorAccess-AWSElasticBeanstalk
- AIDevOpsAgentAccessPolicy
- AIDevOpsAgentActionsPolicy
- AIDevOpsAgentFullAccess
- AIDevOpsAgentReadOnlyAccess
- AIDevOpsOperatorAppAccessPolicy
- AIOpsAssistantIncidentReportPolicy
- AIOpsAssistantPolicy
- AIOpsConsoleAdminPolicy
- AIOpsOperatorAccess
- AIOpsReadOnlyAccess
- AlexaForBusinessDeviceSetup
- AlexaForBusinessFullAccess
- AlexaForBusinessGatewayExecution
- AlexaForBusinessLifesizeDelegatedAccessPolicy
- AlexaForBusinessNetworkProfileServicePolicy
- AlexaForBusinessPolyDelegatedAccessPolicy
- AlexaForBusinessReadOnlyAccess
- AmazonAPIGatewayAdministrator
- AmazonAPIGatewayInvokeFullAccess
- AmazonAPIGatewayPushToCloudWatchLogs

- AmazonAppFlowFullAccess
- AmazonAppFlowReadOnlyAccess
- AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy
- AmazonAppStreamFullAccess
- AmazonAppStreamPCAAccess
- AmazonAppStreamReadOnlyAccess
- AmazonAppStreamServiceAccess
- AmazonAthenaFullAccess
- AmazonAthenaServiceRolePolicy
- AmazonAugmentedAIFullAccess
- AmazonAugmentedAIHumanLoopFullAccess
- AmazonAugmentedAIIntegratedAPIAccess
- AmazonAuroraDSQLConsoleFullAccess
- AmazonAuroraDSQLFullAccess
- AmazonAuroraDSQLReadOnlyAccess
- AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy
- AmazonBedrockExternalWebSearchFullAccess
- AmazonBedrockExternalWebSearchReadOnly
- AmazonBedrockFullAccess
- AmazonBedrockLimitedAccess
- AmazonBedrockMantleFullAccess
- AmazonBedrockMantleInferenceAccess
- AmazonBedrockMantleReadOnly
- AmazonBedrockMarketplaceAccess
- AmazonBedrockReadOnly
- AmazonBedrockStudioPermissionsBoundary
- AmazonBedrockWebSearchFullAccess
- AmazonBedrockWebSearchReadOnly
- AmazonBraketFullAccess

- AmazonBraketJobsExecutionPolicy
- AmazonBraketServiceRolePolicy
- AmazonChimeFullAccess
- AmazonChimeReadOnly
- AmazonChimeSDK
- AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy
- AmazonChimeSDKMessagingServiceRolePolicy
- AmazonChimeServiceRolePolicy
- AmazonChimeTranscriptionServiceLinkedRolePolicy
- AmazonChimeUserManagement
- AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- AmazonCloudDirectoryFullAccess
- AmazonCloudDirectoryReadOnlyAccess
- AmazonCloudWatchEvidentlyFullAccess
- AmazonCloudWatchEvidentlyReadOnlyAccess
- AmazonCloudWatchEvidentlyServiceRolePolicy
- AmazonCloudWatchRUMFullAccess
- AmazonCloudWatchRUMReadOnlyAccess
- AmazonCloudWatchRUMServiceRolePolicy
- AmazonCodeCatalystFullAccess
- AmazonCodeCatalystReadOnlyAccess
- AmazonCodeCatalystSupportAccess
- AmazonCodeGuruProfilerAgentAccess
- AmazonCodeGuruProfilerFullAccess
- AmazonCodeGuruProfilerReadOnlyAccess
- AmazonCodeGuruReviewerFullAccess
- AmazonCodeGuruReviewerReadOnlyAccess
- AmazonCodeGuruReviewerServiceRolePolicy
- AmazonCodeGuruSecurityFullAccess

- AmazonCodeGuruSecurityScanAccess
- AmazonCognitoDeveloperAuthenticatedIdentities
- AmazonCognitoIdpEmailServiceRolePolicy
- AmazonCognitoIdpServiceRolePolicy
- AmazonCognitoPowerUser
- AmazonCognitoReadOnly
- AmazonCognitoUnAuthedIdentitiesSessionPolicy
- AmazonCognitoUnauthenticatedIdentities
- AmazonConnect_FullAccess
- AmazonConnectCampaignsServiceLinkedRolePolicy
- AmazonConnectReadOnlyAccess
- AmazonConnectServiceLinkedRolePolicy
- AmazonConnectSynchronizationServiceRolePolicy
- AmazonConnectVoiceIDFullAccess
- AmazonDataZoneBedrockModelConsumptionPolicy
- AmazonDataZoneBedrockModelManagementPolicy
- AmazonDataZoneDomainExecutionRolePolicy
- AmazonDataZoneEnvironmentRolePermissionsBoundary
- AmazonDataZoneFullAccess
- AmazonDataZoneFullUserAccess
- AmazonDataZoneGlueManageAccessRolePolicy
- AmazonDataZonePortalFullAccessPolicy
- AmazonDataZonePreviewConsoleFullAccess
- AmazonDataZoneProjectDeploymentPermissionsBoundary
- AmazonDataZoneProjectRolePermissionsBoundary
- AmazonDataZoneRedshiftGlueProvisioningPolicy
- AmazonDataZoneRedshiftManageAccessRolePolicy
- AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- AmazonDataZoneSageMakerManageAccessRolePolicy

- AmazonDataZoneSageMakerProvisioningRolePolicy
- AmazonDetectiveFullAccess
- AmazonDetectiveInvestigatorAccess
- AmazonDetectiveMemberAccess
- AmazonDetectiveOrganizationsAccess
- AmazonDetectiveServiceLinkedRolePolicy
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruOrganizationsAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruServiceRolePolicy
- AmazonDMSCloudWatchLogsRole
- AmazonDMSRedshiftS3Role
- AmazonDMSVPCManagementRole
- AmazonDocDB-ElasticServiceRolePolicy
- AmazonDocDBConsoleFullAccess
- AmazonDocDBElasticFullAccess
- AmazonDocDBElasticReadOnlyAccess
- AmazonDocDBFullAccess
- AmazonDocDBReadOnlyAccess
- AmazonDRSVPCManagement
- AmazonDynamoDBFullAccess
- AmazonDynamoDBFullAccess_v2
- AmazonDynamoDBFullAccesswithDataPipeline
- AmazonDynamoDBReadOnlyAccess
- AmazonEBSCSIDriverEKSClusterScopedPolicy
- AmazonEBSCSIDriverPolicy
- AmazonEBSCSIDriverPolicyV2
- AmazonEC2ContainerRegistryFullAccess

- AmazonEC2ContainerRegistryPowerUser
- AmazonEC2ContainerRegistryPullOnly
- AmazonEC2ContainerRegistryReadOnly
- AmazonEC2ContainerServiceAutoscaleRole
- AmazonEC2ContainerServiceEventsRole
- AmazonEC2ContainerServiceforEC2Role
- AmazonEC2ContainerServiceRole
- AmazonEC2FullAccess
- AmazonEC2ImageReferencesAccessPolicy
- AmazonEC2ReadOnlyAccess
- AmazonEC2RoleforAWSCodeDeploy
- AmazonEC2RoleforAWSCodeDeployLimited
- AmazonEC2RoleforDataPipelineRole
- AmazonEC2RoleforSSM
- AmazonEC2RolePolicyForLaunchWizard
- AmazonEC2SpotFleetAutoscaleRole
- AmazonEC2SpotFleetTaggingRole
- AmazonECS_FullAccess
- AmazonECSComputeServiceRolePolicy
- AmazonECSInfrastructureRoleforExpressGatewayServices
- AmazonECSInfrastructureRolePolicyForLoadBalancers
- AmazonECSInfrastructureRolePolicyForManagedInstances
- AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity
- AmazonECSInfrastructureRolePolicyForVolumes
- AmazonECSInfrastructureRolePolicyForVpcLattice
- AmazonECSInstanceRolePolicyForManagedInstances
- AmazonECSServiceRolePolicy
- AmazonECSTaskExecutionRolePolicy
- AmazonEFSCSIDriverPolicy
- AmazonEKS_CNI_Policy

- AmazonEKSBlockStoragePolicy
- AmazonEKSBlockStoragePolicyV2
- AmazonEKSClusterPolicy
- AmazonEKSComputePolicy
- AmazonEKSConnectorServiceRolePolicy
- AmazonEKSDashboardConsoleReadOnly
- AmazonEKSDashboardServiceRolePolicy
- AmazonEKSFargatePodExecutionRolePolicy
- AmazonEKSForFargateServiceRolePolicy
- AmazonEKSLoadBalancingPolicy
- AmazonEKSLocalOutpostClusterPolicy
- AmazonEKSLocalOutpostServiceRolePolicy
- AmazonEKSMCPReadOnlyAccess
- AmazonEKSNetworkingPolicy
- AmazonEKSServicePolicy
- AmazonEKSServiceRolePolicy
- AmazonEKSVPCResourceController
- AmazonEKSWorkerNodeMinimalPolicy
- AmazonEKSWorkerNodePolicy
- AmazonElastiCacheFullAccess
- AmazonElastiCacheReadOnlyAccess
- AmazonElasticContainerRegistryPublicFullAccess
- AmazonElasticContainerRegistryPublicPowerUser
- AmazonElasticContainerRegistryPublicReadOnly
- AmazonElasticFileSystemClientFullAccess
- AmazonElasticFileSystemClientReadOnlyAccess
- AmazonElasticFileSystemClientReadWriteAccess
- AmazonElasticFileSystemFullAccess
- AmazonElasticFileSystemReadOnlyAccess
- AmazonElasticFileSystemServiceRolePolicy

- AmazonElasticFileSystemsUtils
- AmazonElasticMapReduceEditorsRole
- AmazonElasticMapReduceforAutoScalingRole
- AmazonElasticMapReduceforEC2Role
- AmazonElasticMapReduceFullAccess
- AmazonElasticMapReducePlacementGroupPolicy
- AmazonElasticMapReduceReadOnlyAccess
- AmazonElasticMapReduceRole
- AmazonElasticsearchServiceRolePolicy
- AmazonElasticTranscoder_FullAccess
- AmazonElasticTranscoder_JobsSubmitter
- AmazonElasticTranscoder_ReadOnlyAccess
- AmazonElasticTranscoderRole
- AmazonEMRCleanupPolicy
- AmazonEMRContainersServiceRolePolicy
- AmazonEMRFullAccessPolicy_v2
- AmazonEMRReadOnlyAccessPolicy_v2
- AmazonEMRServerlessServiceRolePolicy
- AmazonEMRServicePolicy_v2
- AmazonEMRServicePolicyForSessions
- AmazonESCognitoAccess
- AmazonESFullAccess
- AmazonESReadOnlyAccess
- AmazonEventBridgeApiDestinationsServiceRolePolicy
- AmazonEventBridgeFullAccess
- AmazonEventBridgePipesFullAccess
- AmazonEventBridgePipesOperatorAccess
- AmazonEventBridgePipesReadOnlyAccess
- AmazonEventBridgeReadOnlyAccess
- AmazonEventBridgeSchedulerFullAccess

- AmazonEventBridgeSchedulerReadOnlyAccess
- AmazonEventBridgeSchemasFullAccess
- AmazonEventBridgeSchemasReadOnlyAccess
- AmazonEventBridgeSchemasServiceRolePolicy
- AmazonEVSServiceRolePolicy
- AmazonFISServiceRolePolicy
- AmazonForecastFullAccess
- AmazonFraudDetectorFullAccessPolicy
- AmazonFreeRTOSFullAccess
- AmazonFreeRTOSOTAUpdate
- AmazonFSxConsoleFullAccess
- AmazonFSxConsoleReadOnlyAccess
- AmazonFSxFullAccess
- AmazonFSxReadOnlyAccess
- AmazonFSxServiceRolePolicy
- AmazonGlacierFullAccess
- AmazonGlacierReadOnlyAccess
- AmazonGrafanaAthenaAccess
- AmazonGrafanaCloudWatchAccess
- AmazonGrafanaRedshiftAccess
- AmazonGrafanaServiceLinkedRolePolicy
- AmazonGuardDutyFullAccess
- AmazonGuardDutyFullAccess_v2
- AmazonGuardDutyMalwareProtectionServiceRolePolicy
- AmazonGuardDutyReadOnlyAccess
- AmazonGuardDutyServiceRolePolicy
- AmazonHealthLakeFullAccess
- AmazonHealthLakeReadOnlyAccess
- AmazonHoneycodeFullAccess
- AmazonHoneycodeReadOnlyAccess

- AmazonHoneycodeServiceRolePolicy
- AmazonHoneycodeTeamAssociationFullAccess
- AmazonHoneycodeTeamAssociationReadOnlyAccess
- AmazonHoneycodeWorkbookFullAccess
- AmazonHoneycodeWorkbookReadOnlyAccess
- AmazonInspector2AgentlessServiceRolePolicy
- AmazonInspector2AmiScanServiceRolePolicy
- AmazonInspector2FullAccess
- AmazonInspector2FullAccess_v2
- AmazonInspector2ManagedCisPolicy
- AmazonInspector2ManagedTelemetryPolicy
- AmazonInspector2ReadOnlyAccess
- AmazonInspector2ServiceRolePolicy
- AmazonInspector2ThirdPartyServiceRolePolicy
- AmazonInspectorFullAccess
- AmazonInspectorReadOnlyAccess
- AmazonInspectorServiceRolePolicy
- AmazonKendraFullAccess
- AmazonKendraReadOnlyAccess
- AmazonKeyspacesFullAccess
- AmazonKeyspacesReadOnlyAccess
- AmazonKeyspacesReadOnlyAccess_v2
- AmazonKinesisAnalyticsFullAccess
- AmazonKinesisAnalyticsReadOnly
- AmazonKinesisFirehoseFullAccess
- AmazonKinesisFirehoseReadOnlyAccess
- AmazonKinesisFullAccess
- AmazonKinesisReadOnlyAccess
- AmazonKinesisVideoStreamsFullAccess
- AmazonKinesisVideoStreamsReadOnlyAccess

- AmazonLaunchWizard_Fullaccess
- AmazonLaunchWizardFullAccessV2
- AmazonLexChannelsAccess
- AmazonLexFullAccess
- AmazonLexReadOnly
- AmazonLexReplicationPolicy
- AmazonLexRunBotsOnly
- AmazonLexV2BotPolicy
- AmazonLookoutEquipmentFullAccess
- AmazonLookoutEquipmentReadOnlyAccess
- AmazonLookoutMetricsFullAccess
- AmazonLookoutMetricsReadOnlyAccess
- AmazonLookoutVisionConsoleFullAccess
- AmazonLookoutVisionConsoleReadOnlyAccess
- AmazonLookoutVisionFullAccess
- AmazonLookoutVisionReadOnlyAccess
- AmazonMachineLearningBatchPredictionsAccess
- AmazonMachineLearningCreateOnlyAccess
- AmazonMachineLearningFullAccess
- AmazonMachineLearningManageRealTimeEndpointOnlyAccess
- AmazonMachineLearningReadOnlyAccess
- AmazonMachineLearningRealTimePredictionOnlyAccess
- AmazonMachineLearningRoleforRedshiftDataSourceV3
- AmazonMacieFullAccess
- AmazonMacieHandshakeRole
- AmazonMacieReadOnlyAccess
- AmazonMacieServiceRole
- AmazonMacieServiceRolePolicy
- AmazonManagedBlockchainConsoleFullAccess
- AmazonManagedBlockchainFullAccess

- AmazonManagedBlockchainReadOnlyAccess
- AmazonManagedBlockchainServiceRolePolicy
- AmazonMCSFullAccess
- AmazonMCSReadOnlyAccess
- AmazonMechanicalTurkFullAccess
- AmazonMechanicalTurkReadOnly
- AmazonMemoryDBFullAccess
- AmazonMemoryDBReadOnlyAccess
- AmazonMobileAnalyticsFinancialReportAccess
- AmazonMobileAnalyticsFullAccess
- AmazonMobileAnalyticsNon-financialReportAccess
- AmazonMobileAnalyticsWriteOnlyAccess
- AmazonMonitronFullAccess
- AmazonMQApiFullAccess
- AmazonMQApiReadOnlyAccess
- AmazonMQFullAccess
- AmazonMQReadOnlyAccess
- AmazonMQServiceRolePolicy
- AmazonMSKConnectReadOnlyAccess
- AmazonMSKFullAccess
- AmazonMSKReadOnlyAccess
- AmazonMWAAServerlessServiceRolePolicy
- AmazonMWAAServiceRolePolicy
- AmazonNimbleStudio-LaunchProfileWorker
- AmazonNimbleStudio-StudioAdmin
- AmazonNimbleStudio-StudioUser
- AmazonODBFullAccess
- AmazonODBServiceRolePolicy
- AmazonOmicsFullAccess
- AmazonOmicsReadOnlyAccess

- AmazonOneEnterpriseFullAccess
- AmazonOneEnterpriseInstallerAccess
- AmazonOneEnterpriseReadOnlyAccess
- AmazonOpenSearchDashboardsServiceRolePolicy
- AmazonOpenSearchDirectQueryGlueCreateAccess
- AmazonOpenSearchIngestionFullAccess
- AmazonOpenSearchIngestionReadOnlyAccess
- AmazonOpenSearchIngestionServiceRolePolicy
- AmazonOpenSearchServerlessServiceRolePolicy
- AmazonOpenSearchServiceCognitoAccess
- AmazonOpenSearchServiceFullAccess
- AmazonOpenSearchServiceReadOnlyAccess
- AmazonOpenSearchServiceRolePolicy
- AmazonPersonalizeFullAccess
- AmazonPollyFullAccess
- AmazonPollyReadOnlyAccess
- AmazonPrometheusConsoleFullAccess
- AmazonPrometheusFullAccess
- AmazonPrometheusQueryAccess
- AmazonPrometheusRemoteWriteAccess
- AmazonPrometheusScraperServiceRolePolicy
- AmazonQDeveloperAccess
- AmazonQFullAccess
- AmazonQLDBConsoleFullAccess
- AmazonQLDBFullAccess
- AmazonQLDBReadOnly
- AmazonRDSBetaServiceRolePolicy
- AmazonRDSCustomInstanceProfileRolePolicy
- AmazonRDSCustomPreviewServiceRolePolicy
- AmazonRDSCustomServiceRolePolicy

- AmazonRDSDataFullAccess
- AmazonRDSDirectoryServiceAccess
- AmazonRDSEnhancedMonitoringRole
- AmazonRDSFullAccess
- AmazonRDSPerformanceInsightsFullAccess
- AmazonRDSPerformanceInsightsReadOnly
- AmazonRDSPreviewServiceRolePolicy
- AmazonRDSReadOnlyAccess
- AmazonRDSServiceRolePolicy
- AmazonRedshiftAllCommandsFullAccess
- AmazonRedshiftDataFullAccess
- AmazonRedshiftFederatedAuthorization
- AmazonRedshiftFullAccess
- AmazonRedshiftQueryEditor
- AmazonRedshiftQueryEditorV2FullAccess
- AmazonRedshiftQueryEditorV2NoSharing
- AmazonRedshiftQueryEditorV2ReadSharing
- AmazonRedshiftQueryEditorV2ReadWriteSharing
- AmazonRedshiftReadOnlyAccess
- AmazonRedshiftServiceLinkedRolePolicy
- AmazonRekognitionCustomLabelsFullAccess
- AmazonRekognitionFullAccess
- AmazonRekognitionReadOnlyAccess
- AmazonRekognitionServiceRole
- AmazonRoute53AutoNamingFullAccess
- AmazonRoute53AutoNamingReadOnlyAccess
- AmazonRoute53AutoNamingRegistrantAccess
- AmazonRoute53DomainsFullAccess
- AmazonRoute53DomainsReadOnlyAccess
- AmazonRoute53FullAccess

- AmazonRoute53GlobalResolverFullAccess
- AmazonRoute53GlobalResolverReadOnlyAccess
- AmazonRoute53ProfilesFullAccess
- AmazonRoute53ProfilesReadOnlyAccess
- AmazonRoute53ReadOnlyAccess
- AmazonRoute53RecoveryClusterFullAccess
- AmazonRoute53RecoveryClusterReadOnlyAccess
- AmazonRoute53RecoveryControlConfigFullAccess
- AmazonRoute53RecoveryControlConfigReadOnlyAccess
- AmazonRoute53RecoveryReadinessFullAccess
- AmazonRoute53RecoveryReadinessReadOnlyAccess
- AmazonRoute53ResolverFullAccess
- AmazonRoute53ResolverReadOnlyAccess
- AmazonS3ExpressFullAccess
- AmazonS3ExpressReadOnlyAccess
- AmazonS3FilesClientFullAccess
- AmazonS3FilesClientReadOnlyAccess
- AmazonS3FilesClientReadWriteAccess
- AmazonS3FilesCSIDriverPolicy
- AmazonS3FilesFullAccess
- AmazonS3FilesReadOnlyAccess
- AmazonS3FullAccess
- AmazonS3ObjectLambdaExecutionRolePolicy
- AmazonS3OutpostsFullAccess
- AmazonS3OutpostsReadOnlyAccess
- AmazonS3ReadOnlyAccess
- AmazonS3TablesFullAccess
- AmazonS3TablesLakeFormationServiceRole
- AmazonS3TablesReadOnlyAccess
- AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

- AmazonSageMakerCanvasAIServicesAccess
- AmazonSageMakerCanvasBedrockAccess
- AmazonSageMakerCanvasDataPrepFullAccess
- AmazonSageMakerCanvasDirectDeployAccess
- AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy
- AmazonSageMakerCanvasForecastAccess
- AmazonSageMakerCanvasFullAccess
- AmazonSageMakerCanvasSMDataScienceAssistantAccess
- AmazonSageMakerCapacityReservationServiceRolePolicy
- AmazonSageMakerClusterInstanceRolePolicy
- AmazonSageMakerCoreServiceRolePolicy
- AmazonSageMakerEdgeDeviceFleetPolicy
- AmazonSageMakerFeatureStoreAccess
- AmazonSageMakerFullAccess
- AmazonSageMakerGeospatialExecutionRole
- AmazonSageMakerGeospatialFullAccess
- AmazonSageMakerGroundTruthExecution
- AmazonSageMakerHyperPodGatedModelAccess
- AmazonSageMakerHyperPodInferenceAccess
- AmazonSageMakerHyperPodObservabilityAdminAccess
- AmazonSageMakerHyperPodServiceRolePolicy
- AmazonSageMakerHyperPodTrainingOperatorAccess
- AmazonSageMakerInferenceServiceRolePolicy
- AmazonSageMakerJobFullAccess
- AmazonSageMakerJobRuntimeAccess
- AmazonSageMakerMechanicalTurkAccess
- AmazonSageMakerModelCustomizationCoreAccess
- AmazonSageMakerModelGovernanceUseAccess
- AmazonSageMakerModelRegistryFullAccess
- AmazonSageMakerNotebooksServiceRolePolicy

- AmazonSageMakerPartnerAppsFullAccess
- AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerPipelinesIntegrations
- AmazonSageMakerQuickSightVPCPolicy
- AmazonSageMakerReadOnly
- AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerSpacesControllerPolicy
- AmazonSageMakerSpacesRouterPolicy
- AmazonSageMakerTrainingPlanCreateAccess
- AmazonSecurityLakeAdministrator
- AmazonSecurityLakeMetastoreManager
- AmazonSecurityLakePermissionsBoundary
- AmazonSESFullAccess
- AmazonSESReadOnlyAccess
- AmazonSESServiceRolePolicy
- AmazonSNSFullAccess
- AmazonSNSReadOnlyAccess
- AmazonSNSRole
- AmazonSQSFullAccess
- AmazonSQSReadOnlyAccess
- AmazonSSMAutomationApproverAccess

- AmazonSSMAutomationRole
- AmazonSSMDirectoryServiceAccess
- AmazonSSMFullAccess
- AmazonSSMMaintenanceWindowRole
- AmazonSSMManagedEC2InstanceDefaultPolicy
- AmazonSSMManagedInstanceCore
- AmazonSSMPatchAssociation
- AmazonSSMReadOnlyAccess
- AmazonSSMServiceRolePolicy
- AmazonSumerianFullAccess
- AmazonTextractFullAccess
- AmazonTextractServiceRole
- AmazonTimestreamConsoleFullAccess
- AmazonTimestreamFullAccess
- AmazonTimestreamInfluxDBFullAccess
- AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess
- AmazonTimestreamInfluxDBServiceRolePolicy
- AmazonTimestreamReadOnlyAccess
- AmazonTranscribeFullAccess
- AmazonTranscribeReadOnlyAccess
- AmazonVerifiedPermissionsFullAccess
- AmazonVerifiedPermissionsReadOnlyAccess
- AmazonVPCCrossAccountNetworkInterfaceOperations
- AmazonVPCFullAccess
- AmazonVPCNetworkAccessAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerPathComponentReadPolicy
- AmazonVPCReadOnlyAccess
- AmazonWorkDocsFullAccess
- AmazonWorkDocsReadOnlyAccess

- AmazonWorkMailEventsServiceRolePolicy
- AmazonWorkMailFullAccess
- AmazonWorkMailMessageFlowFullAccess
- AmazonWorkMailMessageFlowReadOnlyAccess
- AmazonWorkMailReadOnlyAccess
- AmazonWorkSpacesAdmin
- AmazonWorkSpacesApplicationManagerAdminAccess
- AmazonWorkspacesPCAAccess
- AmazonWorkSpacesPoolServiceAccess
- AmazonWorkSpacesSecureBrowserReadOnly
- AmazonWorkSpacesSelfServiceAccess
- AmazonWorkSpacesServiceAccess
- AmazonWorkSpacesThinClientFullAccess
- AmazonWorkSpacesThinClientMonitoringServiceRolePolicy
- AmazonWorkSpacesThinClientReadOnlyAccess
- AmazonWorkSpacesWebReadOnly
- AmazonWorkSpacesWebServiceRolePolicy
- AmazonZocaloFullAccess
- AmazonZocaloReadOnlyAccess
- AmplifyBackendDeployFullAccess
- AnthropicFullAccess
- AnthropicInferenceAccess
- AnthropicLimitedAccess
- AnthropicReadOnlyAccess
- AnthropicSelfHostedEnvironmentAccess
- APIGatewayServiceRolePolicy
- AppIntegrationsServiceLinkedRolePolicy
- ApplicationAutoScalingForAmazonAppStreamAccess
- ApplicationDiscoveryServiceContinuousExportServiceRolePolicy
- AppRunnerNetworkingServiceRolePolicy

- AppRunnerServiceRolePolicy
- AppStudioServiceRolePolicy
- AuroraDsqlServiceLinkedRolePolicy
- AutoScalingConsoleFullAccess
- AutoScalingConsoleReadOnlyAccess
- AutoScalingFullAccess
- AutoScalingNotificationAccessRole
- AutoScalingReadOnlyAccess
- AutoScalingServiceRolePolicy
- AWS-SSM-Automation-DiagnosisBucketPolicy
- AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy
- AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy
- AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy
- AWS-SSM-RemediationAutomation-AdministrationRolePolicy
- AWS-SSM-RemediationAutomation-ExecutionRolePolicy
- AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy
- AWS_ ConfigRole
- AWSAccountActivityAccess
- AWSAccountManagementFullAccess
- AWSAccountManagementReadOnlyAccess
- AWSAccountSettingsManagementRole
- AWSAccountUsageReportAccess
- AWSAgentlessDiscoveryService
- AWSAppConfigServiceRolePolicy
- AWSAppFabricFullAccess
- AWSAppFabricReadOnlyAccess
- AWSAppFabricServiceRolePolicy
- AWSApplicationAutoscalingAppStreamFleetPolicy
- AWSApplicationAutoscalingCassandraTablePolicy
- AWSApplicationAutoscalingComprehendEndpointPolicy

- AWSApplicationAutoScalingCustomResourcePolicy
- AWSApplicationAutoscalingDynamoDBTablePolicy
- AWSApplicationAutoscalingEC2SpotFleetRequestPolicy
- AWSApplicationAutoscalingECSServicePolicy
- AWSApplicationAutoscalingElastiCacheRGPolicy
- AWSApplicationAutoscalingEMRInstanceGroupPolicy
- AWSApplicationAutoscalingKafkaClusterPolicy
- AWSApplicationAutoscalingLambdaConcurrencyPolicy
- AWSApplicationAutoscalingNeptuneClusterPolicy
- AWSApplicationAutoscalingRDSClusterPolicy
- AWSApplicationAutoscalingSageMakerEndpointPolicy
- AWSApplicationAutoscalingWorkSpacesPoolPolicy
- AWSApplicationDiscoveryAgentAccess
- AWSApplicationDiscoveryAgentlessCollectorAccess
- AWSApplicationDiscoveryServiceFullAccess
- AWSApplicationMigrationAgentInstallationPolicy
- AWSApplicationMigrationAgentPolicy
- AWSApplicationMigrationAgentPolicy_v2
- AWSApplicationMigrationConversionServerPolicy
- AWSApplicationMigrationEC2Access
- AWSApplicationMigrationFSxProxyPolicy
- AWSApplicationMigrationFSxProxyVPCPolicy
- AWSApplicationMigrationFullAccess
- AWSApplicationMigrationMGHAccess
- AWSApplicationMigrationNetworkMigrationCustomResource
- AWSApplicationMigrationNetworkMigrationMultiAccount
- AWSApplicationMigrationReadOnlyAccess
- AWSApplicationMigrationReplicationServerPolicy
- AWSApplicationMigrationServiceEc2InstancePolicy
- AWSApplicationMigrationServiceRolePolicy

- AWSApplicationMigrationSSMAccess
- AWSApplicationMigrationVCenterClientPolicy
- AWSAppMeshEnvoyAccess
- AWSAppMeshFullAccess
- AWSAppMeshPreviewEnvoyAccess
- AWSAppMeshPreviewServiceRolePolicy
- AWSAppMeshReadOnly
- AWSAppMeshServiceRolePolicy
- AWSAppRunnerFullAccess
- AWSAppRunnerReadOnlyAccess
- AWSAppRunnerServicePolicyForECRAccess
- AWSAppSyncAdministrator
- AWSAppSyncInvokeFullAccess
- AWSAppSyncPushToCloudWatchLogs
- AWSAppSyncSchemaAuthor
- AWSAppSyncServiceRolePolicy
- AWSArtifactAccountSync
- AWSArtifactAgreementsFullAccess
- AWSArtifactAgreementsReadOnlyAccess
- AWSArtifactComplianceInquiriesFullAccess
- AWSArtifactComplianceInquiriesReadOnlyAccess
- AWSArtifactReportsReadOnlyAccess
- AWSArtifactServiceRolePolicy
- AWSAuditManagerAdministratorAccess
- AWSAuditManagerServiceRolePolicy
- AWSAutoScalingPlansEC2AutoScalingPolicy
- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

- AWSBackupGuardDutyRolePolicyForScans
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupSearchOperatorAccess
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForIndexing
- AWSBackupServiceRolePolicyForItemRestores
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSBackupServiceRolePolicyForScans
- AWSBatchFullAccess
- AWSBatchServiceEventTargetRole
- AWSBatchServiceRole
- AWSBatchServiceRolePolicyForSageMaker
- AWSBCMDataExportsServiceRolePolicy
- AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy
- AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy
- AWSBillingConductorFullAccess
- AWSBillingConductorReadOnlyAccess
- AWSBillingReadOnlyAccess
- AWSBillingServiceRolePolicy
- AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM
- AWSBudgetsActionsWithAWSResourceControlAccess
- AWSBudgetsReadOnlyAccess
- AWSBudgetsSpendLimitMemberRolePolicy
- AWSBugBustFullAccess

- AWSBugBustPlayerAccess
- AWSBugBustServiceRolePolicy
- AWSCertificateManagerFullAccess
- AWSCertificateManagerPrivateCAAuditor
- AWSCertificateManagerPrivateCAFullAccess
- AWSCertificateManagerPrivateCAPrivilegedUser
- AWSCertificateManagerPrivateCAReadOnly
- AWSCertificateManagerPrivateCAUser
- AWSCertificateManagerReadOnly
- AWSChatbotServiceLinkedRolePolicy
- AWSCleanRoomsFullAccess
- AWSCleanRoomsFullAccessNoQuerying
- AWSCleanRoomsMLFullAccess
- AWSCleanRoomsMLReadOnlyAccess
- AWSCleanRoomsReadOnlyAccess
- AWSCleanRoomsServiceRolePolicy
- AWSCloud9Administrator
- AWSCloud9EnvironmentMember
- AWSCloud9ServiceRolePolicy
- AWSCloud9SSMInstanceProfile
- AWSCloud9User
- AWSCloudFormationFullAccess
- AWSCloudFormationReadOnlyAccess
- AWSCloudFrontLogger
- AWSCloudFrontVPCOriginServiceRolePolicy
- AWSCloudHSMFullAccess
- AWSCloudHSMReadOnlyAccess
- AWSCloudHSMRole
- AWSCloudMapDiscoverInstanceAccess
- AWSCloudMapFullAccess

- AWSCloudMapReadOnlyAccess
- AWSCloudMapRegisterInstanceAccess
- AWSCloudShellFullAccess
- AWSCloudTrail_FullAccess
- AWSCloudTrail_ReadOnlyAccess
- AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy
- AWSCodeArtifactAdminAccess
- AWSCodeArtifactReadOnlyAccess
- AWSCodeBuildAdminAccess
- AWSCodeBuildDeveloperAccess
- AWSCodeBuildReadOnlyAccess
- AWSCodeCommitFullAccess
- AWSCodeCommitPowerUser
- AWSCodeCommitReadOnly
- AWSCodeDeployDeployerAccess
- AWSCodeDeployFullAccess
- AWSCodeDeployReadOnlyAccess
- AWSCodeDeployRole
- AWSCodeDeployRoleForCloudFormation
- AWSCodeDeployRoleForECS
- AWSCodeDeployRoleForECSLimited
- AWSCodeDeployRoleForLambda
- AWSCodeDeployRoleForLambdaLimited
- AWSCodePipeline_FullAccess
- AWSCodePipeline_ReadOnlyAccess
- AWSCodePipelineApproverAccess
- AWSCodePipelineCustomActionAccess
- AWSCodeStarFullAccess
- AWSCodeStarNotificationsServiceRolePolicy
- AWSCodeStarServiceRole

- AWSCompromisedKeyQuarantine
- AWSCompromisedKeyQuarantineV2
- AWSCompromisedKeyQuarantineV3
- AWSConfigMultiAccountSetupPolicy
- AWSConfigRemediationServiceRolePolicy
- AWSConfigRoleForOrganizations
- AWSConfigRulesExecutionRole
- AWSConfigServiceRolePolicy
- AWSConfigThirdPartyServiceRolePolicy
- AWSConfigUserAccess
- Connettore AWS
- AWSControlTowerAccountServiceRolePolicy
- AWSControlTowerCloudTrailRolePolicy
- AWSControlTowerIdentityCenterManagementPolicy
- AWSControlTowerServiceRolePolicy
- AWSCostAndUsageReportAutomationPolicy
- AWSDataExchangeDataGrantOwnerFullAccess
- AWSDataExchangeDataGrantReceiverFullAccess
- AWSDataExchangeFullAccess
- AWSDataExchangeProviderFullAccess
- AWSDataExchangeReadOnly
- AWSDataExchangeServiceRolePolicyForLicenseManagement
- AWSDataExchangeServiceRolePolicyForOrganizationDiscovery
- AWSDataExchangeSubscriberFullAccess
- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement
- AWSDataLifecycleManagerSSMFullAccess
- AWSDataPipeline_FullAccess
- AWSDataPipeline_PowerUser
- AWSDataSyncDiscoveryServiceRolePolicy

- AWSDataSyncFullAccess
- AWSDataSyncReadOnlyAccess
- AWSDataSyncServiceRolePolicy
- AWSDeadlineCloud-FleetWorker
- AWSDeadlineCloud-UserAccessFarms
- AWSDeadlineCloud-UserAccessFleets
- AWSDeadlineCloud-UserAccessJobs
- AWSDeadlineCloud-UserAccessQueues
- AWSDeadlineCloud-WorkerHost
- AWSDeepLensLambdaFunctionAccessPolicy
- AWSDeepLensServiceRolePolicy
- AWSDeepRacerAccountAdminAccess
- AWSDeepRacerCloudFormationAccessPolicy
- AWSDeepRacerDefaultMultiUserAccess
- AWSDeepRacerFullAccess
- AWSDeepRacerRoboMakerAccessPolicy
- AWSDeepRacerServiceRolePolicy
- AWSDenyAll
- AWSDeviceFarmFullAccess
- AWSDeviceFarmServiceRolePolicy
- AWSDeviceFarmTestGridServiceRolePolicy
- AWSDirectConnectFullAccess
- AWSDirectConnectReadOnlyAccess
- AWSDirectConnectServiceRolePolicy
- AWSDirectoryServiceDataFullAccess
- AWSDirectoryServiceDataReadOnlyAccess
- AWSDirectoryServiceFullAccess
- AWSDirectoryServiceReadOnlyAccess
- AWSDirectoryServiceServiceRolePolicy
- AWSDiscoveryContinuousExportFirehosePolicy

- AWSDMSFleetAdvisorServiceRolePolicy
- AWSDMSServerlessServiceRolePolicy
- AWSEC2CapacityManagerServiceRolePolicy
- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSEC2SqlHaInstancePolicy
- AWSEC2SqlHaServiceRolePolicy
- AWSEC2VssRestorePolicy
- AWSEC2VssSnapshotPolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEKSImageBuild
- AWSElasticBeanstalkEKSObservability
- AWSElasticBeanstalkEKSTagging
- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance
- AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
- AWSElasticBeanstalkManagedUpdatesServiceRolePolicy
- AWSElasticBeanstalkMulticontainerDocker
- AWSElasticBeanstalkReadOnly
- AWSElasticBeanstalkRoleCore
- AWSElasticBeanstalkRoleCWL
- AWSElasticBeanstalkRoleECS
- AWSElasticBeanstalkRoleRDS
- AWSElasticBeanstalkRoleSNS
- AWSElasticBeanstalkRoleWorkerTier
- AWSElasticBeanstalkService
- AWSElasticBeanstalkServiceRolePolicy

- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticDisasterRecoveryAgentInstallationPolicy
- AWSElasticDisasterRecoveryAgentPolicy
- AWSElasticDisasterRecoveryConsoleFullAccess
- AWSElasticDisasterRecoveryConsoleFullAccess_v2
- AWSElasticDisasterRecoveryConversionServerPolicy
- AWSElasticDisasterRecoveryCrossAccountReplicationPolicy
- AWSElasticDisasterRecoveryEc2InstancePolicy
- AWSElasticDisasterRecoveryFailbackInstallationPolicy
- AWSElasticDisasterRecoveryFailbackPolicy
- AWSElasticDisasterRecoveryLaunchActionsPolicy
- AWSElasticDisasterRecoveryNetworkReplicationPolicy
- AWSElasticDisasterRecoveryReadOnlyAccess
- AWSElasticDisasterRecoveryRecoveryInstancePolicy
- AWSElasticDisasterRecoveryReplicationServerPolicy
- AWSElasticDisasterRecoveryServiceRolePolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy_v2
- AWSElasticLoadBalancingClassicServiceRolePolicy
- AWSElasticLoadBalancingServiceRolePolicy
- AWSElementalMediaConnectCreateBridge
- AWSElementalMediaConnectCreateFlow
- AWSElementalMediaConnectDeleteBridge
- AWSElementalMediaConnectDeleteFlow
- AWSElementalMediaConnectFullAccess
- AWSElementalMediaConnectReadOnlyAccess
- AWSElementalMediaConvertFullAccess
- AWSElementalMediaConvertReadOnly
- AWSElementalMediaLiveFullAccess

- AWSElementalMediaLiveReadOnly
- AWSElementalMediaPackageFullAccess
- AWSElementalMediaPackageReadOnly
- AWSElementalMediaPackageV2FullAccess
- AWSElementalMediaPackageV2ReadOnly
- AWSElementalMediaStoreFullAccess
- AWSElementalMediaStoreReadOnly
- AWSElementalMediaTailorFullAccess
- AWSElementalMediaTailorReadOnly
- AWSEnhancedClassicNetworkingMangementPolicy
- AWSEntityResolutionConsoleFullAccess
- AWSEntityResolutionConsoleReadOnlyAccess
- AWSFaultInjectionSimulatorEC2Access
- AWSFaultInjectionSimulatorECSAccess
- AWSFaultInjectionSimulatorEKSAccess
- AWSFaultInjectionSimulatorNetworkAccess
- AWSFaultInjectionSimulatorRDSAccess
- AWSFaultInjectionSimulatorSSMAccess
- AWSFinSpaceServiceRolePolicy
- AWSFMAdminFullAccess
- AWSFMAdminReadOnlyAccess
- AWSFMMemberReadOnlyAccess
- AWSForWordPressPluginPolicy
- AWSGitSyncServiceRolePolicy
- AWSGlobalAcceleratorSLRPolicy
- AWSGlueConsoleFullAccess
- AWSGlueConsoleSageMakerNotebookFullAccess
- AwsGlueDataBrewFullAccessPolicy
- AWSGlueDataBrewServiceRole
- AWSGlueSchemaRegistryFullAccess

- AWSGlueSchemaRegistryReadonlyAccess
- AWSGlueServiceNotebookRole
- AWSGlueServiceRole
- AwsGlueSessionUserRestrictedNotebookPolicy
- AwsGlueSessionUserRestrictedNotebookServiceRole
- AwsGlueSessionUserRestrictedPolicy
- AwsGlueSessionUserRestrictedServiceRole
- AWSGrafanaAccountAdministrator
- AWSGrafanaConsoleReadOnlyAccess
- AWSGrafanaWorkspacePermissionManagement
- AWSGrafanaWorkspacePermissionManagementV2
- AWSGreengrassFullAccess
- AWSGreengrassReadOnlyAccess
- AWSGreengrassResourceAccessRolePolicy
- AWSGroundStationAgentInstancePolicy
- AWSHealth_EventProcessorServiceRolePolicy
- AWSHealthFullAccess
- AWSHealthImagingFullAccess
- AWSHealthImagingReadOnlyAccess
- AWSHealthImagingServiceRolePolicy
- AWSHealthOmicsServiceLinkedRolePolicy
- AWSIAMIdentityCenterAllowListForIdentityContext
- AWSIAMRoleManagerServiceRolePolicy
- AWSIdentityCenterExternalManagementPolicy
- AWSIdentitySyncFullAccess
- AWSIdentitySyncReadOnlyAccess
- AWSImageBuilderFullAccess
- AWSImageBuilderReadOnlyAccess
- AWSImportExportFullAccess
- AWSImportExportReadOnlyAccess

- AWSIncidentManagerIncidentAccessServiceRolePolicy
- AWSIncidentManagerResolverAccess
- AWSIncidentManagerServiceRolePolicy
- AWSIoT1ClickFullAccess
- AWSIoT1ClickReadOnlyAccess
- AWSIoTAnalyticsFullAccess
- AWSIoTAnalyticsReadOnlyAccess
- AWSIoTConfigAccess
- AWSIoTConfigReadOnlyAccess
- AWSIoTDataAccess
- AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction
- AWSIoTDeviceDefenderAudit
- AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction
- AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction
- AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction
- AWSIoTDeviceDefenderUpdateCACertMitigationAction
- AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction
- AWSIoTDeviceTesterForFreeRTOSFullAccess
- AWSIoTDeviceTesterForGreengrassFullAccess
- AWSIoTEventsFullAccess
- AWSIoTEventsReadOnlyAccess
- AWSIoTFleetHubFederationAccess
- AWSIoTFleetwiseServiceRolePolicy
- AWSIoTFullAccess
- AWSIoTLogging
- AWSIoTManagedIntegrationsFullAccess
- AWSIoTManagedIntegrationsRolePolicy
- AWSIoTOTAUpdate
- AWSIotRoboRunnerFullAccess
- AWSIotRoboRunnerReadOnly

- AWSIotRoboRunnerServiceRolePolicy
- AWSIoTRuleActions
- AWSIoTSiteWiseConsoleFullAccess
- AWSIoTSiteWiseFullAccess
- AWSIoTSiteWiseMonitorPortalAccess
- AWSIoTSiteWiseMonitorServiceRolePolicy
- AWSIoTSiteWiseReadOnlyAccess
- AWSIoTThingsRegistration
- AWSIoTTwinMakerServiceRolePolicy
- AWSIoTWirelessDataAccess
- AWSIoTWirelessFullAccess
- AWSIoTWirelessFullPublishAccess
- AWSIoTWirelessGatewayCertManager
- AWSIoTWirelessLogging
- AWSIoTWirelessReadOnlyAccess
- AWSIPAMServiceRolePolicy
- AWSIQContractServiceRolePolicy
- AWSIQFullAccess
- AWSIQPermissionServiceRolePolicy
- AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy
- AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy
- AWSKeyManagementServicePowerUser
- AWSLakeFormationCrossAccountManager
- AWSLakeFormationDataAdmin
- AWSLambda_FullAccess
- AWSLambda_ReadOnlyAccess
- AWSLambdaBasicDurableExecutionRolePolicy
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess

- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB
- AWSLambdaKinesisExecutionRole
- AWSLambdaManagedEC2ResourceOperator
- AWSLambdaMSKExecutionRole
- AWSLambdaNetworkConnectorOperatorPolicy
- AWSLambdaReplicator
- AWSLambdaRole
- AWSLambdaServiceRolePolicy
- AWSLambdaSQSQueueExecutionRole
- AWSLambdaVPCAccessExecutionRole
- AWSLicenseManagerConsumptionPolicy
- AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy
- AWSLicenseManagerMasterAccountRolePolicy
- AWSLicenseManagerMemberAccountRolePolicy
- AWSLicenseManagerServiceRolePolicy
- AWSLicenseManagerUserSubscriptionsServiceRolePolicy
- AWSM2ServicePolicy
- AWSManagedAccountManagementAccess
- AWSManagedAccountUserEntitlementAccess
- AWSManagedAdvancedFeaturesActivationAccess
- AWSManagedBudgetsSpendLimitManagementAccess
- AWSManagedControlPolicyManagementAccess
- AWSManagedServiceAccessManagementAccess
- AWSManagedServices_ContactsServiceRolePolicy
- AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy
- AWSManagedServices_EventsServiceRolePolicy
- AWSManagedServices_SelfServiceReporting_ServiceRolePolicy
- AWSManagedServicesDeploymentToolkitPolicy

- AWSManagedSettingsAdminAccess
- AWSManagedSettingsReadOnlyAccess
- AWSManagedSignUpAdminAccess
- AWSManagementConsoleAdministratorAccess
- AWSManagementConsoleBasicUserAccess
- AWSMarketplaceAmiIngestion
- AWSMarketplaceDeploymentServiceRolePolicy
- AWSMarketplaceDiscoveryFullAccess
- AWSMarketplaceFullAccess
- AWSMarketplaceGetEntitlements
- AWSMarketplaceImageBuildFullAccess
- AWSMarketplaceLicenseManagementServiceRolePolicy
- AWSMarketplaceManageSubscriptions
- AWSMarketplaceMeteringFullAccess
- AWSMarketplaceMeteringRegisterUsage
- AWSMarketplaceProcurementSystemAdminFullAccess
- AWSMarketplacePurchaseOrdersServiceRolePolicy
- AWSMarketplaceRead-only
- AWSMarketplaceResaleAuthorizationServiceRolePolicy
- AWSMarketplaceSellerFullAccess
- AWSMarketplaceSellerOfferManagement
- AWSMarketplaceSellerProductsFullAccess
- AWSMarketplaceSellerProductsReadOnly
- AWSMcpServiceActionsFullAccess
- AWSMCPSignInOAuthAccessPolicy
- AWSMediaConnectServicePolicy
- AWSMediaLiveAnywhereServiceRolePolicy
- AWSMediaTailorServiceRolePolicy
- AWSMigrationHubDiscoveryAccess
- AWSMigrationHubDMSAccess

- AWSMigrationHubFullAccess
- AWSMigrationHubOrchestratorConsoleFullAccess
- AWSMigrationHubOrchestratorInstanceRolePolicy
- AWSMigrationHubOrchestratorPlugin
- AWSMigrationHubOrchestratorServiceRolePolicy
- AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess
- AWSMigrationHubRefactorSpaces-SSMAutomationPolicy
- AWSMigrationHubRefactorSpacesFullAccess
- AWSMigrationHubRefactorSpacesServiceRolePolicy
- AWSMigrationHubSMSAccess
- AWSMigrationHubStrategyCollector
- AWSMigrationHubStrategyConsoleFullAccess
- AWSMigrationHubStrategyServiceRolePolicy
- AWSMobileHub_FullAccess
- AWSMobileHub_ReadOnly
- AWSMSKReplicatorExecutionRole
- AWSNATGatewayServiceRolePolicy
- AWSNetworkFirewallFullAccess
- AWSNetworkFirewallReadOnlyAccess
- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess
- AWSNetworkManagerServiceRolePolicy
- AWSObservabilityAdminLogsCentralizationServiceRolePolicy
- AWSObservabilityAdminServiceRolePolicy
- AWSObservabilityAdminTelemetryEnablementServiceRolePolicy
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy

- AWSOutpostsAuthorizeServerPolicy
- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPartnerCentralChannelHandshakeApprovalManagement
- AWSPartnerCentralChannelManagement
- AWSPartnerCentralFullAccess
- AWSPartnerCentralMarketingManagement
- AWSPartnerCentralOpportunityManagement
- AWSPartnerCentralRevenueAttributionManagement
- AWSPartnerCentralSandboxFullAccess
- AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy
- AWSPartnerLedSupportReadOnlyAccess
- AWSPartnerProServeToolsFullAccess
- AWSPartnerProServeToolsIndividualContributor
- AWSPartnerProServeToolsOrganizationReaderIndividualContributor
- AWSPCSComputeNodePolicy
- AWSPCSServiceRolePolicy
- AWSPriceListServiceFullAccess
- AWSPrivateCAAuditor
- AWSPrivateCAConnectorForKubernetesPolicy
- AWSPrivateCAFullAccess
- AWSPrivateCAPrivilegedUser
- AWSPrivateCAReadOnly
- AWSPrivateCAUser

- AWSPrivateMarketplaceAdminFullAccess
- AWSPrivateMarketplaceRequests
- AWSPrivateNetworksServiceRolePolicy
- AWSProtonCodeBuildProvisioningBasicAccess
- AWSProtonCodeBuildProvisioningServiceRolePolicy
- AWSProtonDeveloperAccess
- AWSProtonFullAccess
- AWSProtonReadOnlyAccess
- AWSProtonServiceGitSyncServiceRolePolicy
- AWSProtonSyncServiceRolePolicy
- AWSPurchaseOrdersServiceRolePolicy
- AWSQuickSetupCFGCPacksPermissionsBoundary
- AWSQuickSetupDeploymentRolePolicy
- AWSQuickSetupDevOpsGuruPermissionsBoundary
- AWSQuickSetupDistributorPermissionsBoundary
- AWSQuickSetupEnableAREXExecutionPolicy
- AWSQuickSetupEnableDHMCExecutionPolicy
- AWSQuickSetupJITNADeploymentRolePolicy
- AWSQuickSetupManagedInstanceProfileExecutionPolicy
- AWSQuickSetupManageJITNAResourcesExecutionPolicy
- AWSQuickSetupPatchPolicyBaselineAccess
- AWSQuickSetupPatchPolicyDeploymentRolePolicy
- AWSQuickSetupPatchPolicyLambdaExecutionPolicy
- AWSQuickSetupPatchPolicyPermissionsBoundary
- AWSQuickSetupPatchPolicyTagManagementExecutionPolicy
- AWSQuickSetupSchedulerPermissionsBoundary
- AWSQuickSetupSSMDeploymentRolePolicy
- AWSQuickSetupSSMDeploymentS3BucketRolePolicy
- AWSQuickSetupSSMHostMgmtPermissionsBoundary
- AWSQuickSetupSSMLifecycleManagementExecutionPolicy

- AWSQuickSetupSSMManageResourcesExecutionPolicy
- AWSQuickSetupStartSSMAssociationsExecutionPolicy
- AWSQuickSetupStartStopInstancesExecutionPolicy
- AWSQuickSightAssetBundleExportPolicy
- AWSQuickSightAssetBundleImportPolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS
- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightSecretsManagerWriteAccess
- AWSQuickSightSecretsManagerWritePolicy
- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess
- AWSRepostSpaceSupportOperationsPolicy
- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResilienceHubResilienceTestingPolicy
- AWSResilienceHubServiceRolePolicy
- AWSResilienceHubV2AssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess
- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess

- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess
- AWSRevenueAttributionManagement
- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereFullAccess
- AWSRolesAnywhereReadOnly
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess
- AWSSDMPServiceRolePolicy
- AWSSecretsManagerClientReadOnlyAccess
- AWSSecurityAgentServiceRolePolicy
- AWSSecurityAgentWebAppPolicy
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSSecurityHubV2ServiceRolePolicy
- AWSSecurityIncidentResponseCaseFullAccess
- AWSSecurityIncidentResponseFullAccess
- AWSSecurityIncidentResponseReadOnlyAccess
- AWSSecurityIncidentResponseServiceRolePolicy
- AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWSServiceCatalogAdminFullAccess

- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess
- AWSServiceCatalogOrgsDataSyncServiceRolePolicy
- AWSServiceCatalogSyncServiceRolePolicy
- AWSServiceRoleForAIDevOpsPolicy
- AWSServiceRoleForAmazonEKSNodegroup
- AWSServiceRoleForAmazonQDeveloper
- AWSServiceRoleForAWSTransform
- AWSServiceRoleForAWSTransformCustom
- AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy
- AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy
- AWSServiceRoleForCodeGuru-Profiler
- AWSServiceRoleForCodeWhispererPolicy
- AWSServiceRoleForEC2ScheduledInstances
- AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy
- AWSServiceRoleForImageBuilder
- AWSServiceRoleForIoTSiteWise
- AWSServiceRoleForLogDeliveryPolicy
- AWSServiceRoleForMonitronPolicy
- AWSServiceRoleForNeptuneGraphPolicy
- AWSServiceRoleForPrivateMarketplaceAdminPolicy
- AWSServiceRoleForProcurementInsightsPolicy
- AWSServiceRoleForSMS
- AWSServiceRoleForUserSubscriptions
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting

- AWSServiceRolePolicyForWorkspacesInstances
- AWSShieldDRTAccessPolicy
- AWSShieldServiceRolePolicy
- AWSSocialMessagingServiceRolePolicy
- AWSSSMForSAPServiceLinkedRolePolicy
- AWSSSMOpsInsightsServiceRolePolicy
- AWSSSODirectoryAdministrator
- AWSSSODirectoryReadOnly
- AWSSSOMasterAccountAdministrator
- AWSSSOMemberAccountAdministrator
- AWSSSOReadOnly
- AWSSSOServiceRolePolicy
- AWSStepFunctionsConsoleFullAccess
- AWSStepFunctionsFullAccess
- AWSStepFunctionsReadOnlyAccess
- AWSStorageGatewayFullAccess
- AWSStorageGatewayReadOnlyAccess
- AWSStorageGatewayServiceRolePolicy
- AWSSupplyChainFederationAdminAccess
- AWSSupportAccess
- AWSSupportAppFullAccess
- AWSSupportAppReadOnlyAccess
- AWSSupportPlansFullAccess
- AWSSupportPlansReadOnlyAccess
- AWSSupportPlansServiceRolePolicy
- AWSSupportServiceRolePolicy
- AWSSystemsManagerAccountDiscoveryServicePolicy
- AWSSystemsManagerChangeManagementServicePolicy
- AWSSystemsManagerEnableConfigRecordingExecutionPolicy
- AWSSystemsManagerEnableExplorerExecutionPolicy

- AWSSystemsManagerForSAPFullAccess
- AWSSystemsManagerForSAPReadOnlyAccess
- AWSSystemsManagerJustInTimeAccessServicePolicy
- AWSSystemsManagerJustInTimeAccessTokenPolicy
- AWSSystemsManagerJustInTimeAccessTokenSessionPolicy
- AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy
- AWSSystemsManagerNotificationsServicePolicy
- AWSSystemsManagerOpsDataSyncServiceRolePolicy
- AWSThinkboxAssetServerPolicy
- AWSThinkboxAWSPortalAdminPolicy
- AWSThinkboxAWSPortalGatewayPolicy
- AWSThinkboxAWSPortalWorkerPolicy
- AWSThinkboxDeadlineResourceTrackerAccessPolicy
- AWSThinkboxDeadlineResourceTrackerAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginWorkerPolicy
- AWSTransferConsoleFullAccess
- AWSTransferFullAccess
- AWSTransferLoggingAccess
- AWSTransferReadOnlyAccess
- AWSTransformApplicationDeploymentPolicy
- AWSTransformApplicationECSDeploymentPolicy
- AWSTransformCustomExecuteTransformations
- AWSTransformCustomFullAccess
- AWSTransformCustomManageTransformations
- AWSTransformInfrastructureExecutorAccessBatch
- AWSTransformInfrastructureExecutorAccessEC2
- AWSTransformRevenueAttributionPolicy
- AWSTransformSecretsManagerConnectorPolicy
- AWSTransformSecurityAgentExecutorAccess

- AWSTrustedAdvisorPriorityFullAccess
- AWSTrustedAdvisorPriorityReadOnlyAccess
- AWSTrustedAdvisorReportingServiceRolePolicy
- AWSTrustedAdvisorServiceRolePolicy
- AWSUserAttributeCostAllocationPolicy
- AWSUserNotificationsServiceLinkedRolePolicy
- AWSVendorInsightsAssessorFullAccess
- AWSVendorInsightsAssessorReadOnly
- AWSVendorInsightsVendorFullAccess
- AWSVendorInsightsVendorReadOnly
- AWSVPCFlowLogsServiceRolePolicy
- AWSVpcLatticeServiceRolePolicy
- AWSVPCS2SVpnServiceRolePolicy
- AWSVPCTransitGatewayServiceRolePolicy
- AWSVPCVerifiedAccessServiceRolePolicy
- AWSWAFConsoleFullAccess
- AWSWAFConsoleReadOnlyAccess
- AWSWAFFullAccess
- AWSWAFReadOnlyAccess
- AWSWellArchitectedDiscoveryServiceRolePolicy
- AWSWellArchitectedOrganizationsServiceRolePolicy
- AWSWickrFullAccess
- AWSXrayCrossAccountSharingConfiguration
- AWSXRayDaemonWriteAccess
- AWSXrayFullAccess
- AWSXrayReadOnlyAccess
- AWSXrayWriteOnlyAccess
- AWSZonalAutoshiftPracticeRunSLRPolicy
- AWSZoneGroupAccessManagementServiceRolePolicy
- BatchServiceRolePolicy

- BedrockAgentCoreFullAccess
- BedrockAgentCoreNetworkServiceRolePolicy
- BedrockAgentCoreRuntimeIdentityServiceRolePolicy
- Fatturazione
- BudgetsServiceRolePolicy
- CertificateManagerServiceRolePolicy
- ClientVPNServiceConnectionsRolePolicy
- ClientVPNServiceRolePolicy
- CloudFormationStackSetsOrgAdminServiceRolePolicy
- CloudFormationStackSetsOrgMemberServiceRolePolicy
- CloudFrontFullAccess
- CloudFrontReadOnlyAccess
- CloudHSMServiceRolePolicy
- CloudSearchFullAccess
- CloudSearchReadOnlyAccess
- CloudTrailEventContext
- CloudTrailServiceRolePolicy
- CloudWatch-CrossAccountAccess
- CloudWatchActionsEC2Access
- CloudWatchAgentAdminPolicy
- CloudWatchAgentServerPolicy
- CloudWatchAPIKeyAccess
- CloudWatchApplicationInsightsFullAccess
- CloudWatchApplicationInsightsReadOnlyAccess
- CloudwatchApplicationInsightsServiceLinkedRolePolicy
- CloudWatchApplicationSignalsFullAccess
- CloudWatchApplicationSignalsReadOnlyAccess
- CloudWatchApplicationSignalsServiceRolePolicy
- CloudWatchAutomaticDashboardsAccess
- CloudWatchCrossAccountSharingConfiguration

- CloudWatchEventsBuiltInTargetExecutionAccess
- CloudWatchEventsFullAccess
- CloudWatchEventsInvocationAccess
- CloudWatchEventsReadOnlyAccess
- CloudWatchEventsServiceRolePolicy
- CloudWatchFullAccess
- CloudWatchFullAccessV2
- CloudWatchInternetMonitorFullAccess
- CloudWatchInternetMonitorReadOnlyAccess
- CloudWatchInternetMonitorServiceRolePolicy
- CloudWatchLambdaApplicationSignalsExecutionRolePolicy
- CloudWatchLambdaInsightsExecutionRolePolicy
- CloudWatchLogsAPIKeyAccess
- CloudWatchLogsCrossAccountSharingConfiguration
- CloudWatchLogsFullAccess
- CloudWatchLogsReadOnlyAccess
- CloudWatchNetworkFlowMonitorAgentPublishPolicy
- CloudWatchNetworkFlowMonitorServiceRolePolicy
- CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy
- CloudWatchNetworkMonitorServiceRolePolicy
- CloudWatchOpenSearchDashboardAccess
- CloudWatchOpenSearchDashboardsFullAccess
- CloudWatchReadOnlyAccess
- CloudWatchSyntheticsFullAccess
- CloudWatchSyntheticsReadOnlyAccess
- ComprehendDataAccessRolePolicy
- ComprehendFullAccess
- ComprehendMedicalFullAccess
- ComprehendReadOnly
- ComputeOptimizerAutomationServiceRolePolicy

- ComputeOptimizerReadOnlyAccess
- ComputeOptimizerServiceRolePolicy
- ConfigConformsServiceRolePolicy
- ConsoleFullAccessFromVercel
- ConsoleViewOnlyAccessFromVercel
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DBModDiscoveryAndAssessment
- DBModProvisioningAndMigration
- DBModVirtualSource
- DeclarativePoliciesEC2Report
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBGlobalTableSettingsManagementServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy
- EC2ApplicationStatusChecksServiceRolePolicy
- EC2FastLaunchFullAccess
- EC2FastLaunchServiceRolePolicy
- EC2FleetTimeShiftableServiceRolePolicy
- Ec2ImageBuilderCrossAccountDistributionAccess
- EC2ImageBuilderExecutionPolicy
- EC2ImageBuilderLifecycleExecutionPolicy
- EC2InstanceConnect
- Ec2InstanceConnectEndpoint
- EC2InstanceProfileForImageBuilder

- EC2InstanceProfileForImageBuilderECRContainerBuilds
- ECRReplicationServiceRolePolicy
- ECRTemplateServiceRolePolicy
- ElastiCacheServiceRolePolicy
- ElasticLoadBalancingFullAccess
- ElasticLoadBalancingReadOnly
- ElementalActivationsDownloadSoftwareAccess
- ElementalActivationsFullAccess
- ElementalActivationsGenerateLicenses
- ElementalActivationsReadOnlyAccess
- ElementalAppliancesSoftwareFullAccess
- ElementalAppliancesSoftwareReadOnlyAccess
- ElementalSupportCenterFullAccess
- EMRDescribeClusterPolicyForEMRWAL
- FinOpsAgentAgentPolicy
- FinOpsAgentOperatorPolicy
- FMSServiceRolePolicy
- FSxDeleteServiceLinkedRoleAccess
- GameLiftContainerFleetPolicy
- GameLiftGameServerGroupPolicy
- GitLabDuoWithAmazonQPermissionsPolicy
- GlobalAcceleratorFullAccess
- GlobalAcceleratorReadOnlyAccess
- GreengrassOTAUpdateArtifactAccess
- GroundTruthSyntheticConsoleFullAccess
- GroundTruthSyntheticConsoleReadOnlyAccess
- Health_OrganizationsServiceRolePolicy
- IAMAccessAdvisorReadOnly
- IAMAccessAnalyzerFullAccess
- IAMAccessAnalyzerReadOnlyAccess

- IAMFullAccess
- IAMReadOnlyAccess
- IAMSelfManageServiceSpecificCredentials
- IAMUserChangePassword
- IAMUserSSHKeys
- IVSFullAccess
- IVSReadOnlyAccess
- IVSRecordToS3
- KafkaConnectServiceRolePolicy
- KafkaServiceRolePolicy
- KeyspacesCDCServiceRolePolicy
- KeyspacesReplicationServiceRolePolicy
- LakeFormationDataAccessServiceRolePolicy
- LexBotPolicy
- LexChannelPolicy
- LightsailExportAccess
- MediaConnectGatewayInstanceRolePolicy
- MediaPackageServiceRolePolicy
- MemoryDBServiceRolePolicy
- MigrationHubDMSAccessServiceRolePolicy
- MigrationHubServiceRolePolicy
- MigrationHubSMSAccessServiceRolePolicy
- MonitronServiceRolePolicy
- MultiPartyApprovalFullAccess
- MultiPartyApprovalReadOnlyAccess
- NeptuneConsoleFullAccess
- NeptuneFullAccess
- NeptuneGraphReadOnlyAccess
- NeptuneReadOnlyAccess
- NetworkAdministrator

- NetworkSecurityDirectorServiceLinkedRolePolicy
- NovaActServiceRolePolicy
- OAMFullAccess
- OAMReadOnlyAccess
- OpensearchIngestionSelfManagedVpcePolicy
- PartnerCentralAccountManagementUserRoleAssociation
- PartnerCentralIncentiveBenefitManagement
- PowerUserAccess
- PricingPlanManagerFullAccess
- PricingPlanManagerReadonlyAccess
- QAppsServiceRolePolicy
- QBusinessQuicksightPluginPolicy
- QBusinessServiceRolePolicy
- QuickSightAccessForS3StorageManagementAnalyticsReadOnly
- RDSCloudHsmAuthorizationRole
- ReadOnlyAccess
- ReInventTicketApprovalAccess
- ResourceGroupsandTagEditorFullAccess
- ResourceGroupsandTagEditorReadOnlyAccess
- ResourceGroupsServiceRolePolicy
- ResourceGroupsTaggingAPITagUntagSupportedResources
- ROSAAmazonEBSCSIDriverOperatorPolicy
- ROSACloudNetworkConfigOperatorPolicy
- ROSAControlPlaneOperatorPolicy
- ROSAImageRegistryOperatorPolicy
- ROSAIngressOperatorPolicy
- ROSAInstallerPolicy
- ROSAKarpenterControllerPolicy
- ROSAKMSProviderPolicy
- ROSAKubeControllerPolicy

- ROSAManageSubscription
- ROSANodePoolManagementPolicy
- ROSASharedVPCEndpointPolicy
- ROSASharedVPCRoute53Policy
- ROSASRESupportPolicy
- ROSAWorkerInstancePolicy
- Route53RecoveryReadinessServiceRolePolicy
- Route53ResolverServiceRolePolicy
- RTBFabricServiceRolePolicy
- S3StorageLensServiceRolePolicy
- SageMakerStudioAdminIAMConsolePolicy
- SageMakerStudioAdminIAMDefaultExecutionPolicy
- SageMakerStudioAdminIAMPermissiveExecutionPolicy
- SageMakerStudioAdminProjectUserRolePolicy
- SageMakerStudioBedrockAgentServiceRolePolicy
- SageMakerStudioBedrockChatAgentUserRolePolicy
- SageMakerStudioBedrockEvaluationJobServiceRolePolicy
- SageMakerStudioBedrockFlowServiceRolePolicy
- SageMakerStudioBedrockFunctionExecutionRolePolicy
- SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy
- SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy
- SageMakerStudioBedrockPromptUserRolePolicy
- SageMakerStudioDomainExecutionRolePolicy
- SageMakerStudioDomainServiceRolePolicy
- SageMakerStudioEMRContainersSystemNamespaceRolePolicy
- SageMakerStudioEMRInstanceRolePolicy
- SageMakerStudioEMRServiceRolePolicy
- SageMakerStudioFullAccess
- SageMakerStudioProjectProvisioningRolePolicy
- SageMakerStudioProjectRoleMachineLearningPolicy

- SageMakerStudioProjectUserRolePermissionsBoundary
- SageMakerStudioProjectUserRolePolicy
- SageMakerStudioQueryExecutionRolePolicy
- SageMakerStudioUserIAMConsolePolicy
- SageMakerStudioUserIAMDefaultExecutionPolicy
- SageMakerStudioUserIAMPermissiveExecutionPolicy
- SecretsManagerReadWrite
- SecurityAgentWebAppAPIPolicy
- SecurityAgentWebAppPolicy
- SecurityAudit
- SecurityLakeResourceManagementServiceRolePolicy
- SecurityLakeServiceLinkedRole
- ServerMigration_ServiceRole
- ServerMigrationConnector
- ServerMigrationServiceConsoleFullAccess
- ServerMigrationServiceLaunchRole
- ServerMigrationServiceRoleForInstanceValidation
- ServiceQuotasFullAccess
- ServiceQuotasReadOnlyAccess
- ServiceQuotasServiceRolePolicy
- SignInLocalDevelopmentAccess
- SimpleWorkflowFullAccess
- SMSVoiceServiceRolePolicy
- SplitCostAllocationDataServiceRolePolicy
- SSMQuickSetupRolePolicy
- SupportUser
- SystemAdministrator
- TranslateFullAccess
- TranslateReadOnly
- ViewOnlyAccess

- VMImportExportRoleForAWSConnector
- VPCLatticeFullAccess
- VPCLatticeReadOnlyAccess
- VPCLatticeServicesInvokeAccess
- WAFLoggingServiceRolePolicy
- WAFRegionalLoggingServiceRolePolicy
- WAFV2LoggingServiceRolePolicy
- WellArchitectedAgentResourceScanning
- WellArchitectedConsoleFullAccess
- WellArchitectedConsoleReadOnlyAccess
- WorkLinkServiceRolePolicy

AccessAnalyzerServiceRolePolicy

Descrizione: consenti ad Access Analyzer di analizzare i metadati delle risorse

`AccessAnalyzerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 2 dicembre 2019, 17:13 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Versione della politica

Versione della politica: v23 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessAnalyzerServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ecr:DescribeRepositories",
        "ecr:GetAccountSetting",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListEntitiesForPolicy",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetUser",
        "iam:GetGroup",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails",
        "iam:ListAccessKeys",
        "iam:GetLoginProfile",
        "iam:GetAccessKeyLastUsed",
```

```
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListUserPolicies",
        "iam:GetUserPolicy",
        "iam:ListAttachedUserPolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListGroupsForUser",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListVersionsByFunction",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
```

```
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "sns:GetTopicAttributes",
        "sns:ListTopics",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AccountAccessManagerServiceRolePolicy

Descrizione: concede al gestore degli accessi all'account le autorizzazioni per gestire l'accesso Account AWS

`AccountAccessManagerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 29 giugno 2026, 19:12 UTC
- Ora modificata: 29 giugno 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccountAccessManagerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeAccount",
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AccountManagementFromVercel

Descrizione: Da utilizzare con account creati tramite l'integrazione di Vercel Marketplace con AWS. Fornisce accesso alla gestione degli account, alle notifiche, all'analisi dei costi e dell'utilizzo e alla gestione dei provider di identità.

`AccountManagementFromVercel`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AccountManagementFromVercel` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2025, 16:34 UTC
- Ora modificata: 07 maggio 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AccountManagementFromVercel`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:CloseAccount",
        "bcm-recommended-actions:ListRecommendedActions",
        "ce:GetCostAndUsage",
        "cur:GetUsageReport",
        "iam:ListSAMLProviders",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSamlProvider",
        "iam:GetSamlProvider"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}"
        }
      }
    },
    {
      "Sid" : "ManageServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:DeleteRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/Vercel/Service_2026_04_16",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}",
          "iam:PermissionsBoundary" : [
            "arn:aws:iam::partner:policy/permissions-boundary/vercel.com/
VercelMarketplaceServiceRoleBoundary_2026_04_16"
          ]
        }
      }
    },
    {
      "Sid" : "TagManageServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Vercel/Service_2026_04_16",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AdministratorAccess

Descrizione: fornisce l'accesso completo a AWS servizi e risorse.

`AdministratorAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AdministratorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 6 febbraio 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AdministratorAccess-Amplify

Descrizione: concede le autorizzazioni amministrative dell'account consentendo esplicitamente l'accesso diretto alle risorse necessarie alle applicazioni Amplify.

`AdministratorAccess-Amplify`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AdministratorAccess-Amplify` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 19:03 UTC
- Ora modificata: 04 aprile 2024, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CLICloudformationPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
```

```
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackSet",
        "cloudformation:UpdateStackSet",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*"
      ]
    },
    {
      "Sid" : "CLIManageviaCFNPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:UpdateRole",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:PassRole",
        "iam:ListPolicyVersions",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:CreateRole",
        "iam:ListRolePolicies",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary",
```

```
        "appsync:CreateApiKey",
        "appsync:CreateDataSource",
        "appsync:CreateFunction",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteApiKey",
        "appsync:DeleteDataSource",
        "appsync:DeleteFunction",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetDataSource",
        "appsync:GetFunction",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetType",
        "appsync:GraphQL",
        "appsync:ListApiKeys",
        "appsync:ListDataSources",
        "appsync:ListFunctions",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListResolversByFunction",
        "appsync:ListTypes",
        "appsync:StartSchemaCreation",
        "appsync:UntagResource",
        "appsync:UpdateApiKey",
        "appsync:UpdateDataSource",
        "appsync:UpdateFunction",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:CreateGraphqlApi",
        "appsync:DeleteGraphqlApi",
        "appsync:GetGraphqlApi",
        "appsync:ListTagsForResource",
        "appsync:UpdateGraphqlApi",
        "apigateway:DELETE",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "cognito-idp:CreateUserPool",
        "cognito-identity:CreateIdentityPool",
```

```
        "cognito-identity:DeleteIdentityPool",
        "cognito-identity:DescribeIdentity",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:UpdateIdentityPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:CreateGroup",
        "cognito-idp:DeleteGroup",
        "cognito-identity:TagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:SetUserPoolMfaConfig",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeAsync",
        "lambda:InvokeFunction",
        "lambda:RemovePermission",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:AddLayerVersionPermission",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteLayerVersion",
        "lambda:GetEventSourceMapping",
        "lambda:GetLayerVersion",
        "lambda:ListEventSourceMappings",
        "lambda:ListLayerVersions",
        "lambda:PublishLayerVersion",
        "lambda:RemoveLayerVersionPermission",
        "lambda:UpdateEventSourceMapping",
```

```
        "dynamodb:CreateTable",
        "dynamodb:DeleteItem",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListStreams",
        "dynamodb:PutItem",
        "dynamodb:TagResource",
        "dynamodb:ListTagsOfResource",
        "dynamodb:UntagResource",
        "dynamodb:UpdateContinuousBackups",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable",
        "dynamodb:UpdateTimeToLive",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketWebsite",
        "s3:PutObjectAcl",
        "cloudfront:CreateCloudFrontOriginAccessIdentity",
        "cloudfront:CreateDistribution",
        "cloudfront:DeleteCloudFrontOriginAccessIdentity",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudfront:UpdateCloudFrontOriginAccessIdentity",
        "cloudfront:UpdateDistribution",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "mobiletargeting:GetApp",
        "kinesis:AddTagsToStream",
        "kinesis:CreateStream",
```

```
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListTagsForStream",
        "kinesis:PutRecords",
        "es:AddTags",
        "es:CreateElasticsearchDomain",
        "es:DeleteElasticsearchDomain",
        "es:DescribeElasticsearchDomain",
        "es:UpdateElasticsearchDomainConfig",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CLISDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetIntrospectionSchema",
        "appsync:GraphQL",
        "appsync:UpdateApiKey",
        "appsync:ListApiKeys",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "sts:AssumeRole",
        "mobiletargeting:*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:CreateGroup",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUser",
        "cognito-idp:ListUsers",
        "cognito-idp:AdminGetUser",
        "cognito-idp:ListUsersInGroup",
        "cognito-idp:AdminDisableUser",
```

```
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:AdminResetUserPassword",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:ListGroups",
        "cognito-idp:AdminListUserAuthEvents",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminConfirmSignUp",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminUpdateUserAttributes",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:AdminSetUserPassword",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:DeleteIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "lambda:GetFunction",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:DeleteLayerVersion",
        "lambda:InvokeFunction",
        "lambda:ListLayerVersions",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListPolicyVersions",
        "iam:ListAttachedRolePolicies",
        "iam:CreateRole",
        "iam:PassRole",
        "iam:ListRolePolicies",
```

```
        "iam:DeleteRolePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "sns:CreateSMSSandboxPhoneNumber",
        "sns:GetSMSSandboxAccountStatus",
        "sns:VerifySMSSandboxPhoneNumber",
        "sns:DeleteSMSSandboxPhoneNumber",
        "sns:ListSMSSandboxPhoneNumbers",
        "sns:ListOriginationNumbers",
        "rekognition:DescribeCollection",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "lex:GetBot",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "cloudformation:GetTemplateSummary",
        "codecommit:GitPull",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "polly:DescribeVoices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSMCalls",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*"
    },
    {
      "Sid" : "GeoPowerUser",
      "Effect" : "Allow",
```

```
      "Action" : [
        "geo:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyEcrSDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyStorageSDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteBucketWebsite",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSRCalls",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudfront:CreateCloudFrontOriginAccessIdentity",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByLambdaFunction",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListInvalidations",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListStreamingDistributions",
        "cloudfront:UpdateDistribution",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudfront:ListTagsForResource",
        "cloudfront:DeleteDistribution",
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:PutRolePolicy",
        "iam:PassRole",
        "lambda:CreateFunction",
        "lambda:EnableReplication",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "s3:CreateBucket",
        "s3:GetAccelerateConfiguration",
        "s3:GetObject",
        "s3:ListBucket",
```

```
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutObject",
        "s3:PutBucketTagging",
        "s3:GetBucketTagging",
        "lambda:ListEventSourceMappings",
        "lambda:CreateEventSourceMapping",
        "iam:UpdateAssumeRolePolicy",
        "iam:DeleteRolePolicy",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:UpdateApp",
        "amplify:UpdateBranch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSRViewLogGroups",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "arn:aws:logs:*:*:log-group:*"
    },
    {
      "Sid" : "AmplifySSRCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*"
    },
    {
      "Sid" : "AmplifySSRPushLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*:log-stream:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AdministratorAccess-AWSElasticBeanstalk

Descrizione: concede le autorizzazioni amministrative dell'account. Consente esplicitamente a sviluppatori e amministratori di accedere direttamente alle risorse necessarie per gestire le applicazioni Elastic AWS Beanstalk

`AdministratorAccess-AWSElasticBeanstalk`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AdministratorAccess-AWSElasticBeanstalk` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 gennaio 2021, 19:36 UTC
- Ora modificata: 19 maggio 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:Validate*",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "codecommit:Get*",
        "codecommit:UploadArchive",
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate*",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroup*",
        "ecs:CreateCluster",
        "ecs:DeRegisterTaskDefinition",
        "ecs:Describe*",
        "ecs:List*",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:Describe*",
        "iam:GetRole",
```

```
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "logs:Describe*",
        "rds:Describe*",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:*"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CancelUpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:SignalResource",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/Elastic-Beanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:TagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/awseb-e-*",
        "arn:aws:dynamodb:*:*:table/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*Rule",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetSecurityGroups"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*"
      ],
```

```
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/eb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/awseb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/eb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/eb-*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-elasticbeanstalk*",
        "arn:aws:iam::*:instance-profile/aws-elasticbeanstalk*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk*",
      "Condition" : {
        "ArnLike" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::aws:policy/AWSElasticBeanstalk*",
            "arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalk*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/autoscaling.amazonaws.com/
AWSServiceRoleForAutoScaling",
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk",
        "arn:aws:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing",
        "arn:aws:iam::*:role/aws-service-role/
managedupdates.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk",
        "arn:aws:iam::*:role/aws-service-role/
maintenance.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "elasticbeanstalk.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "managedupdates.elasticbeanstalk.amazonaws.com",
            "maintenance.elasticbeanstalk.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*DBSubnetGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBInstance",
        "rds:DeleteDBSecurityGroup",
        "rds:ModifyDBInstance",
        "rds:RestoreDBInstanceFromDBSnapshot"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:secgrp:eb-*",
        "arn:aws:rds:*:*:snapshot:*",
        "arn:aws:rds:*:*:subgrp:awseb-e-*",
        "arn:aws:rds:*:*:subgrp:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
```

```
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:*QueueAttributes",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:SendMessage",
        "sqs:TagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AIDevOpsAgentAccessPolicy

Descrizione: fornisce le autorizzazioni richieste dall' AWS DevOps agente per condurre indagini ed eseguire analisi sulle risorse dei clienti AWS .

`AIDevOpsAgentAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AIDevOpsAgentAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 marzo 2026, 03:42 UTC
- Ora modificata: 02 luglio 2026, 23:42 UTC

- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentAccessPolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOPSServiceWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:StartQuery",
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIOPSServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:GetCertificate",
        "acm:ListCertificates",
        "aidevops:GetAsset",
        "aidevops:GetAssetContent",
        "aidevops:GetAssetFile",
```

```
        "aidevops:GetKnowledgeItem",
        "aidevops:ListAssetFiles",
        "aidevops:ListAssets",
        "aidevops:ListAssetTypes",
        "aidevops:ListAssetVersions",
        "aidevops:ListKnowledgeItems",
        "airflow:List*",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetFunction",
        "appsync:GetGraphqlApi",
        "appsync:GetGraphqlApiEnvironmentVariables",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
```

```
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:List*",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:List*",
        "bcm-data-exports:Get*",
        "bcm-data-exports:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetFoundationModel",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetProvisionedModelThroughput",
```

```
        "bedrock:List*",
        "budgets:Describe*",
        "budgets:List*",
        "budgets:ViewBudget",
        "ce:Describe*",
        "ce:Get*",
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:List*",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:List*",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Describe*",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
```

```
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetInsightRuleReport",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetService",
        "cloudwatch:GetServiceLevelObjective",
        "cloudwatch:List*",
        "codeartifact:Describe*",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:List*",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentTarget",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:List*",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:List*",
```

```
        "codestar-notifications:Describe*",
        "codestar-notifications:List*",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListTagsForResource",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "connect:Describe*",
        "connect:GetTaskTemplate",
        "connect:List*",
        "cur:Describe*",
        "cur:Get*",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:Describe*",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:List*",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
```

```
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetStorageProfile",
        "deadline:List*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:GetResourceCollection",
        "devops-guru:List*",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeHostedConnections",
        "directconnect:DescribeInterconnects",
        "directconnect:DescribeLags",
        "directconnect:DescribeTags",
        "directconnect:DescribeVirtualInterfaces",
        "dms:Describe*",
        "dms:List*",
        "ds:Describe*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:Describe*",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetCapacityManagerAttributes",
        "ec2:GetCapacityManagerMetricData",
        "ec2:GetCapacityManagerMonitoredTagKeys",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
```

```
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:Describe*",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:AccessKubernetesApi",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:GetResourcePolicy",
        "elasticloadbalancing:GetTrustStoreCaCertificatesBundle",
        "elasticloadbalancing:GetTrustStoreRevocationContent",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
        "emr-serverless:GetApplication",
        "emr-serverless:List*",
        "es:Describe*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:List*",
        "firehose:Describe*",
        "firehose:List*",
```

```
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:List*",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "frauddetector:BatchGetVariable",
        "frauddetector:Describe*",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetJobs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
```

```
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:List*",
        "glue:querySchemaVersionMetadata",
        "grafana:Describe*",
        "grafana:List*",
        "greengrass:Describe*",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:List*",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:Describe*",
        "healthlake:List*",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
```

```
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccountAliases",
        "iam:ListAttachedRolePolicies",
        "iam:ListOpenIDConnectProviders",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:List*",
        "inspector2:List*",
        "inspector2:SearchVulnerabilities",
        "inspector:Describe*",
        "inspector:List*",
        "internetmonitor:GetMonitor",
        "internetmonitor:List*",
        "iot:Describe*",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotevents:Describe*",
        "iotevents:List*",
```

```
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:List*",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:List*",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:List*",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeKey",
        "kms:ListResourceTags",
        "kms:ListKeys",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeyRotations",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:GetResourceLFTags",
```

```
        "lakeformation:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "license-manager:GetLicense",
        "license-manager:List*",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
```

```
        "logs:List*",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:List*",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
        "macie2:List*",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
```

```
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:List*",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:List*",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:List*",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pi:Describe*",
        "pi:Get*",
        "pi:List*",
```

```
        "pipes:Describe*",
        "pipes:List*",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
        "proton:List*",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:List*",
        "ram:GetPermission",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:Get*",
        "resiliencehub:List*",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
```

```
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:List*",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHealthCheckStatus",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:List*",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
```

```
            "s3:GetBucketPolicy",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketTagging",
            "s3:GetBucketVersioning",
            "s3:GetEncryptionConfiguration",
            "s3:GetIntelligentTieringConfiguration",
            "s3:GetInventoryConfiguration",
            "s3:GetLifecycleConfiguration",
            "s3:GetMultiRegionAccessPoint",
            "s3:GetMultiRegionAccessPointPolicy",
            "s3:GetMultiRegionAccessPointPolicyStatus",
            "s3:GetReplicationConfiguration",
            "s3:GetStorageLensConfiguration",
            "s3:GetStorageLensConfigurationTagging",
            "s3:GetStorageLensGroup",
            "s3:ListAllMyBuckets",
            "sagemaker:Describe*",
            "sagemaker:List*",
            "scheduler:GetSchedule",
            "scheduler:GetScheduleGroup",
            "scheduler:List*",
            "schemas:Describe*",
            "schemas:GetResourcePolicy",
            "schemas:List*",
            "secretsmanager:Describe*",
            "secretsmanager:GetResourcePolicy",
            "secretsmanager:List*",
            "securityhub:BatchGetAutomationRules",
            "securityhub:BatchGetSecurityControls",
            "securityhub:Describe*",
            "securityhub:GetConfigurationPolicy",
            "securityhub:GetConfigurationPolicyAssociation",
            "securityhub:GetEnabledStandards",
            "securityhub:GetFindingAggregator",
            "securityhub:GetFindings",
            "securityhub:GetInsights",
            "securityhub:List*",
            "securitylake:GetSubscriber",
            "securitylake:List*",
            "servicecatalog:Describe*",
            "servicecatalog:GetApplication",
            "servicecatalog:GetAttributeGroup",
            "servicecatalog:List*",
            "servicequotas:Get*",
```

```
        "servicequotas:List*",
        "ses:Describe*",
        "ses:GetAccount",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
        "signer:GetSigningProfile",
        "signer:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:List*",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "ssm:Describe*",
        "ssm:GetCommandInvocation",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
```

```
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:GetSharedSsoConfiguration",
        "sso:ListAccountAssignments",
        "sso:ListApplicationAssignments",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:GetExecutionHistory",
        "states:Describe*",
        "states:List*",
        "support:DescribeCases",
        "synthetics:Describe*",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:List*",
        "tag:GetResources",
        "timestream:Describe*",
        "timestream:List*",
        "transfer:Describe*",
        "transfer:List*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:List*",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
```

```
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:List*",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:List*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:BatchGetTraces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIOPSAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
```

```
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AIDevOpsAgentActionsPolicy

Descrizione: fornisce le autorizzazioni elevate richieste dall' AWS DevOps agente per eseguire mutazioni o azioni elevate approvate dall'operatore sulle risorse del cliente durante gli eventi operativi. AWS

`AIDevOpsAgentActionsPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AIDevOpsAgentActionsPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 giugno 2026, 22:27 UTC

- Ora modificata: 23 giugno 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentActionsPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIDevOpsMutativeAccess",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "cloudformation:UpdateStack",
        "cloudwatch:PutMetricAlarm",
        "ec2:CreateTags",
        "ec2:ModifyInstanceAttribute",
        "ecs:UpdateService",
        "elasticloadbalancing:ModifyTargetGroup",
        "lambda:UpdateFunctionConfiguration",
        "logs:PutMetricFilter",
        "rds:ModifyDBInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AIDevOpsAgentFullAccess

Descrizione: Fornisce l'accesso completo ad Amazon DevOps Agent tramite Console di gestione AWS

`AIDevOpsAgentFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AIDevOpsAgentFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 marzo 2026, 03:42 UTC
- Ora modificata: 26 giugno 2026, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIDevOpsAgentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:AllowVendedLogDeliveryForResource",
```

```
            "aidevops:AssociateService",
            "aidevops:CreateAccessToken",
            "aidevops:CreateAgentSpace",
            "aidevops:CreateAsset",
            "aidevops:CreateAssetFile",
            "aidevops:CreateBacklogTask",
            "aidevops:CreateChat",
            "aidevops:CreateKnowledgeItem",
            "aidevops:CreateOneTimeLoginSession",
            "aidevops:CreatePrivateConnection",
            "aidevops:CreateTrigger",
            "aidevops:DeleteAgentSpace",
            "aidevops:DeleteAsset",
            "aidevops:DeleteAssetFile",
            "aidevops:DeleteKnowledgeItem",
            "aidevops:DeletePrivateConnection",
            "aidevops:DeleteTrigger",
            "aidevops:DeregisterService",
            "aidevops:DescribePrivateConnection",
            "aidevops:DescribeServices",
            "aidevops:DescribeSupportLevel",
            "aidevops:DisableOperatorApp",
            "aidevops:DisassociateService",
            "aidevops:DiscoverTopology",
            "aidevops:EnableOperatorApp",
            "aidevops:EndChatForCase",
            "aidevops:GetAccessToken",
            "aidevops:GetAccountUsage",
            "aidevops:GetAgentSpace",
            "aidevops:GetAsset",
            "aidevops:GetAssetContent",
            "aidevops:GetAssetFile",
            "aidevops:GetAssociation",
            "aidevops:GetBacklogTask",
            "aidevops:GetKnowledgeItem",
            "aidevops:GetOperatorApp",
            "aidevops:GetRecommendation",
            "aidevops:GetService",
            "aidevops:GetTrigger",
            "aidevops:InitiateChatForCase",
            "aidevops:ListAccessTokens",
            "aidevops:ListAgentSpaces",
            "aidevops:ListAssetFiles",
            "aidevops:ListAssets",
```

```
        "aidevops:ListAssetTypes",
        "aidevops:ListAssetVersions",
        "aidevops:ListAssociations",
        "aidevops:ListBacklogTasks",
        "aidevops:ListChats",
        "aidevops:ListExecutions",
        "aidevops:ListGoals",
        "aidevops:ListJournalRecords",
        "aidevops:ListKnowledgeItems",
        "aidevops:ListKnowledgeItemVersions",
        "aidevops:ListPendingMessages",
        "aidevops:ListPrivateConnections",
        "aidevops:ListRecommendations",
        "aidevops:ListServices",
        "aidevops:ListTagsForResource",
        "aidevops:ListTriggers",
        "aidevops:ListWebhooks",
        "aidevops:RegisterService",
        "aidevops:RevokeAccessToken",
        "aidevops:RotateAccessToken",
        "aidevops:SearchServiceAccessibleResource",
        "aidevops:SendMessage",
        "aidevops:TagResource",
        "aidevops:UntagResource",
        "aidevops:UpdateAgentSpace",
        "aidevops:UpdateApprovalAction",
        "aidevops:UpdateAsset",
        "aidevops:UpdateAssetFile",
        "aidevops:UpdateAssociation",
        "aidevops:UpdateBacklogTask",
        "aidevops:UpdateGoal",
        "aidevops:UpdateKnowledgeItem",
        "aidevops:UpdateOperatorAppIdpConfig",
        "aidevops:UpdatePrivateConnectionCertificate",
        "aidevops:UpdateRecommendation",
        "aidevops:UpdateTrigger",
        "aidevops:ValidateAwsAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AIDevOpsAgentReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon DevOps Agent tramite Console di gestione AWS

`AIDevOpsAgentReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AIDevOpsAgentReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 marzo 2026, 03:42 UTC
- Ora modificata: 11 giugno 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AIDevOpsAgentReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:DescribePrivateConnection",
        "aidevops:DescribeServices",
        "aidevops:Get*",
        "aidevops:List*",
        "aidevops:SearchServiceAccessibleResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AIDevOpsOperatorAppAccessPolicy

Descrizione: fornisce l'accesso all'utilizzo dell'app Web AWS DevOps dell'operatore per un Agent Space.

`AIDevOpsOperatorAppAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AIDevOpsOperatorAppAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 marzo 2026, 03:42 UTC
- Ora modificata: 26 giugno 2026, 23:57 UTC

- ARN: `arn:aws:iam::aws:policy/AIDevOpsOperatorAppAccessPolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOperatorAgentSpaceActions",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:CreateAccessToken",
        "aidevops:CreateAsset",
        "aidevops:CreateAssetFile",
        "aidevops:CreateBacklogTask",
        "aidevops:CreateChat",
        "aidevops:CreateKnowledgeItem",
        "aidevops:CreateTrigger",
        "aidevops:DeleteAsset",
        "aidevops:DeleteAssetFile",
        "aidevops:DeleteKnowledgeItem",
        "aidevops:DeleteTrigger",
        "aidevops:DescribeServices",
        "aidevops:DescribeSupportLevel",
        "aidevops:DiscoverTopology",
        "aidevops:EndChatForCase",
        "aidevops:GetAccessToken",
        "aidevops:GetAgentSpace",
        "aidevops:GetAsset",
        "aidevops:GetAssetContent",
        "aidevops:GetAssetFile",
        "aidevops:GetAssociation",
        "aidevops:GetBacklogTask",
        "aidevops:GetKnowledgeItem",
```

```
        "aidevops:GetRecommendation",
        "aidevops:GetTrigger",
        "aidevops:InitiateChatForCase",
        "aidevops:ListAccessTokens",
        "aidevops:ListAssetFiles",
        "aidevops:ListAssets",
        "aidevops:ListAssetTypes",
        "aidevops:ListAssetVersions",
        "aidevops:ListAssociations",
        "aidevops:ListBacklogTasks",
        "aidevops:ListChats",
        "aidevops:ListExecutions",
        "aidevops:ListGoals",
        "aidevops:ListJournalRecords",
        "aidevops:ListKnowledgeItems",
        "aidevops:ListKnowledgeItemVersions",
        "aidevops:ListPendingMessages",
        "aidevops:ListRecommendations",
        "aidevops:ListTriggers",
        "aidevops:RevokeAccessToken",
        "aidevops:RotateAccessToken",
        "aidevops:SendMessage",
        "aidevops:UpdateApprovalAction",
        "aidevops:UpdateAsset",
        "aidevops:UpdateAssetFile",
        "aidevops:UpdateBacklogTask",
        "aidevops:UpdateGoal",
        "aidevops:UpdateKnowledgeItem",
        "aidevops:UpdateRecommendation",
        "aidevops:UpdateTrigger"
      ],
      "Resource" : "arn:aws:aidevops:*:*:agentspace/${aws:PrincipalTag/AgentSpaceId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorAccountActions",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:GetAccountUsage"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSupportOperatorActions",
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeServices",
        "support:InitiateChatForCase",
        "support:DescribeSupportLevel"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSecretsManagerOperatorActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowTranscribeOperatorActions",
      "Effect" : "Allow",
      "Action" : [
        "transcribe:StartStreamTranscriptionWebSocket"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AIOpsAssistantIncidentReportPolicy

Descrizione: fornisce le autorizzazioni richieste da Amazon AI Operations Assistant per generare il rapporto sugli incidenti dell'indagine.

`AIOpsAssistantIncidentReportPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AIOpsAssistantIncidentReportPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 ottobre 2025, 22:04 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantIncidentReportPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GetReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "aiops:GetFact",
        "aiops:ListFacts",
        "aiops:GetFactVersions",
        "aiops:GetInvestigation",
        "aiops:ListInvestigationEvents",
        "aiops:GetInvestigationEvent"
      ],
      "Resource" : [
        "arn:aws:aiops:*:*:investigation-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AIOpsAssistantPolicy

Descrizione: fornisce ReadOnly le autorizzazioni richieste da Amazon AI Operations Assistant per eseguire analisi sulle AWS risorse dei clienti durante le indagini.

`AIOpsAssistantPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AIOpsAssistantPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 dicembre 2024, 16:21 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantPolicy`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOPSServiceAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "airflow:List*",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetFunction",
```

```
        "appsync:GetGraphqlApi",
        "appsync:GetGraphqlApiEnvironmentVariables",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:List*",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:List*",
        "budgets:Describe*",
        "budgets:List*",
```

```
        "ce:Describe*",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:List*",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:List*",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Describe*",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetResourcePolicy",
```

```
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartQuery",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetInsightRuleReport",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetService",
        "cloudwatch:GetServiceLevelObjective",
        "cloudwatch:List*",
        "codeartifact:Describe*",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:List*",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:List*",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:List*",
        "codestar-notifications:Describe*",
        "codestar-notifications:List*",
        "cognito-identity:DescribeIdentityPool",
```

```
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListTagsForResource",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "connect:Describe*",
        "connect:GetTaskTemplate",
        "connect:List*",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:Describe*",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:List*",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
```

```
        "deadline:GetStorageProfile",
        "deadline:List*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:GetResourceCollection",
        "devops-guru:List*",
        "dms:Describe*",
        "dms:List*",
        "ds:Describe*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:Describe*",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:Describe*",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
```

```
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:GetResourcePolicy",
        "elasticloadbalancing:GetTrustStoreCaCertificatesBundle",
        "elasticloadbalancing:GetTrustStoreRevocationContent",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
        "emr-serverless:GetApplication",
        "emr-serverless:List*",
        "es:Describe*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:List*",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "frauddetector:BatchGetVariable",
        "frauddetector:Describe*",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
```

```
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetJob",
        "glue:GetRegistry",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:List*",
        "glue:querySchemaVersionMetadata",
        "grafana:Describe*",
        "grafana:List*",
        "greengrass:Describe*",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:List*",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:List*",
        "health:DescribeEvents",
        "health:DescribeEventDetails",
        "healthlake:Describe*",
        "healthlake:List*",
        "iam:GetGroup",
```

```
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListOpenIDConnectProviders",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:List*",
        "inspector2:List*",
        "inspector:Describe*",
        "inspector:List*",
        "internetmonitor:GetMonitor",
        "internetmonitor:List*",
        "iot:Describe*",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
```

```
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotevents:Describe*",
        "iotevents:List*",
        "iotfleethub:Describe*",
        "iotfleethub:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:List*",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:List*",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:List*",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeKey",
```

```
        "kms:ListResourceTags",
        "kms:ListKeys",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeyRotations",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:GetResourceLFTags",
        "lakeformation:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "lex:Describe*",
        "lex:List*",
        "license-manager:GetLicense",
        "license-manager:List*",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
```

```
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:List*",
        "lookoutvision:Describe*",
        "lookoutvision:List*",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:List*",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
        "macie2:List*",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
```

```
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
        "nimble:GetLaunchProfile",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:List*",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:List*",
        "opsworks-cm:Describe*",
```

```
        "opsworks-cm:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:List*",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:List*",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:Describe*",
        "pipes:List*",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
        "proton:List*",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:List*",
        "qldb:Describe*",
        "qldb:List*",
        "ram:GetPermission",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
```

```
        "redshift:Describe*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:List*",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:List*",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:List*",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
```

```
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:List*",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:List*",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "S3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
```

```
            "s3:GetStorageLensConfiguration",
            "s3:GetStorageLensConfigurationTagging",
            "s3:GetStorageLensGroup",
            "s3:List*",
            "sagemaker:Describe*",
            "sagemaker:List*",
            "scheduler:GetSchedule",
            "scheduler:GetScheduleGroup",
            "scheduler:List*",
            "schemas:Describe*",
            "schemas:GetResourcePolicy",
            "schemas:List*",
            "secretsmanager:Describe*",
            "secretsmanager:GetResourcePolicy",
            "secretsmanager:List*",
            "securityhub:BatchGetAutomationRules",
            "securityhub:BatchGetSecurityControls",
            "securityhub:Describe*",
            "securityhub:GetConfigurationPolicy",
            "securityhub:GetConfigurationPolicyAssociation",
            "securityhub:GetEnabledStandards",
            "securityhub:GetFindingAggregator",
            "securityhub:GetInsights",
            "securityhub:List*",
            "securitylake:GetSubscriber",
            "securitylake:List*",
            "servicecatalog:Describe*",
            "servicecatalog:GetApplication",
            "servicecatalog:GetAttributeGroup",
            "servicecatalog:List*",
            "servicequotas:GetServiceQuota",
            "ses:Describe*",
            "ses:GetAccount",
            "ses:GetAddonInstance",
            "ses:GetAddonSubscription",
            "ses:GetArchive",
            "ses:GetConfigurationSet",
            "ses:GetConfigurationSetEventDestinations",
            "ses:GetContactList",
            "ses:GetDedicatedIpPool",
            "ses:GetDedicatedIps",
            "ses:GetEmailIdentity",
            "ses:GetEmailTemplate",
            "ses:GetIngressPoint",
```

```
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
        "signer:GetSigningProfile",
        "signer:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:List*",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "ssm:Describe*",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:GetSharedSsoConfiguration",
        "sso:ListAccountAssignments",
        "sso:ListApplicationAssignments",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListTagsForResource",
```

```
        "states:GetExecutionHistory",
        "states:Describe*",
        "states:List*",
        "synthetics:Describe*",
        "synthetics:GetCanary",
        "synthetics:GetGroup",
        "synthetics:List*",
        "tag:GetResources",
        "timestream:Describe*",
        "timestream:List*",
        "transfer:Describe*",
        "transfer:List*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:List*",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:List*",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:List*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
```

```
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:BatchGetTraces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIOPSS3AccessForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amplify",
        "arn:aws:s3:::cdk--assets--*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ViaAWSService" : [
            "amplify.amazonaws.com"
          ],
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "AIOPSAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
```

```
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AIOpsConsoleAdminPolicy

Descrizione: concede l'accesso completo al servizio Amazon AI Operations e alle relative autorizzazioni richieste tramite AWS console. Include anche le autorizzazioni per utilizzare sessioni di console con riconoscimento dell'identità.

`AIOpsConsoleAdminPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AIOpsConsoleAdminPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 dicembre 2024, 23:51 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsConsoleAdminPolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "aiops:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        }
      }
    },
    {
      "Sid" : "SSOApplicationTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:TagResource"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/aiops"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:RequestTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
      "Sid" : "SSOTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:TagResource"
      ],
```

```
      "Resource" : "arn:aws:sso::*:application/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:ListApplications",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:DescribeInstance",
        "sso:GetSSOStatus",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "IdentityPropagationAccess",
      "Effect" : "Allow",
      "Action" : [
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CloudtrailAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListEventDataStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMIntegrationSecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:aws/ssm/3p/*"
    },
    {
      "Sid" : "SSMIntegrationAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationCreatePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
```

```
      "Resource" : "arn:aws:iam::*:policy/service-role/
AWSServiceRoleSSMIntegrationsPolicy*"
    },
    {
      "Sid" : "ChatbotConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackWorkspaces",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListMicrosoftTeamsConfiguredTeams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleToAIOps",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "aiops.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagBoundaryPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "IAMPassRoleToSSMIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.integrations.amazonaws.com"
        },
        "ArnEquals" : {
          "iam:AssociatedResourceArn" : "arn:aws:aiops:*:*:investigation-group/*"
        }
      }
    },
    {
      "Sid" : "SSMOpsItemAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:*:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : "CloudWatch",
          "aws:ResourceTag/Integration" : "CloudWatch"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Integration"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAIOpsCrossAccountAssistantPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/AIOpsCrossAccountAssistantPolicy*"
    },
```

```
    {
      "Sid" : "AmazonQAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AIOpsOperatorAccess

Descrizione: concede l'accesso ad Amazon AI Operations APIs per creare, aggiornare ed eliminare indagini, eventi investigativi e risorse investigative. Include anche ReadOnly l'accesso a tutte le operazioni di intelligenza artificiale APIs e l'utilizzo di sessioni con riconoscimento dell'identità.

`AIOpsOperatorAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AIOpsOperatorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 2 dicembre 2024, 23:51 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsOperatorAccess`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsOperatorAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:CreateInvestigation",
        "aiops:CreateInvestigationEvent",
        "aiops:CreateInvestigationResource",
        "aiops:DeleteInvestigation",
        "aiops:Get*",
        "aiops:List*",
        "aiops:UpdateInvestigation",
        "aiops:UpdateInvestigationEvent",
        "aiops:ValidateInvestigationGroup",
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMSettingServiceIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationTagAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "Integration"
        }
      }
    },
    {
      "Sid" : "SSMOpsItemIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        }
      }
    },
    {
      "Sid" : "SSMTagOperation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Integration"
        }
      }
    },
    {
      "Sid" : "SSMOpsSummaryIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AIOpsReadOnlyAccess

Descrizione: concede ReadOnly le autorizzazioni al servizio Amazon AI Operations e alle relative risorse richieste.

`AIOpsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AIOpsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 dicembre 2024, 23:51 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:Get*",
        "aiops:List*",
        "aiops:ValidateInvestigationGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AlexaForBusinessDeviceSetup

Descrizione: Fornisci l'accesso ai AlexaForBusiness servizi per la configurazione del dispositivo

`AlexaForBusinessDeviceSetup`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AlexaForBusinessDeviceSetup` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:47 UTC
- Ora modificata: 20 maggio 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterDevice",
        "a4b:CompleteRegistration",
        "a4b:SearchDevices",
        "a4b:SearchNetworkProfiles",
        "a4b:GetNetworkProfile",
        "a4b:PutDeviceSetupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "A4bDeviceSetupAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AlexaForBusinessFullAccess

Descrizione: garantisce l'accesso completo alle AlexaForBusiness risorse e l'accesso alle risorse correlate Servizi AWS

`AlexaForBusinessFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AlexaForBusinessFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:47 UTC
- Ora modificata: 01 luglio 2020, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:*",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "*a4b.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*a4b.amazonaws.com/
AWSServiceRoleForAlexaForBusiness*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4B*"
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "A4B*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AlexaForBusinessGatewayExecution

Descrizione: Fornisci l'accesso di esecuzione del gateway ai AlexaForBusiness servizi

`AlexaForBusinessGatewayExecution`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AlexaForBusinessGatewayExecution` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:47 UTC

- Ora modificata: 30 novembre 2017, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Send*",
        "a4b:Get*"
      ],
      "Resource" : "arn:aws:a4b:*:*:gateway/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:dd-*",
        "arn:aws:sqs:*:*:sd-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:List*",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:DescribeLogGroups",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AlexaForBusinessLifesizeDelegatedAccessPolicy

Descrizione: Fornisci l'accesso ai dispositivi Lifesize AVS

`AlexaForBusinessLifesizeDelegatedAccessPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AlexaForBusinessLifesizeDelegatedAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 giugno 2020, 19:46 UTC
- Ora modificata: 12 giugno 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A2IWO7UEGWV4TL"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "a4b:filters_deviceType" : [
            "*A2IWO7UEGWV4TL"
          ]
        },
        "Null" : {
          "a4b:filters_deviceType" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:GetRoom",
        "a4b:GetAddressBook",
        "a4b:SearchRooms",
        "a4b:CreateContact",
        "a4b:CreateRoom",
        "a4b:UpdateContact",
        "a4b:ListConferenceProviders",
        "a4b:DeleteRoom",
        "a4b:CreateAddressBook",
        "a4b:DisassociateContactFromAddressBook",
        "a4b:CreateConferenceProvider",
        "a4b:PutConferencePreference",
        "a4b:DeleteAddressBook",
        "a4b:AssociateContactWithAddressBook",
        "a4b:DeleteContact",
        "a4b:SearchProfiles",
        "a4b:UpdateProfile",
        "a4b:GetContact"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AlexaForBusinessNetworkProfileServicePolicy

Descrizione: questa politica consente ad Alexa for Business di eseguire attività automatizzate pianificate dai tuoi profili di rete.

`AlexaForBusinessNetworkProfileServicePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 13 marzo 2019, 00:53 UTC
- Ora modificata: 5 aprile 2019, 21:57 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "A4bPcaTagAccess",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate",
        "acm-pca:RevokeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/a4b" : "enabled"
        }
      }
    },
    {
      "Sid" : "A4bNetworkProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AlexaForBusinessPolyDelegatedAccessPolicy

Descrizione: Fornisci l'accesso ai dispositivi Poly AVS

`AlexaForBusinessPolyDelegatedAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AlexaForBusinessPolyDelegatedAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 ottobre 2019, 19:48 UTC
- Ora modificata: 16 ottobre 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
```

```
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD"
      ]
    },
    {
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A238TWV36W3S92",
            "A1FUZ1SC53VJXD"
          ]
        }
      }
    },
    {
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
```

```
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
      "Action" : [
        "a4b:GetRoom",
        "a4b:SearchRooms",
        "a4b:CreateRoom",
        "a4b:GetProfile",
        "a4b:SearchSkillGroups",
        "a4b:DisassociateSkillGroupFromRoom",
        "a4b:AssociateSkillGroupWithRoom",
        "a4b:GetSkillGroup",
        "a4b:SearchProfiles",
        "a4b:GetAddressBook",
        "a4b:UpdateRoom"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AlexaForBusinessReadOnlyAccess

Descrizione: Fornisci l'accesso in sola lettura ai AlexaForBusiness servizi

`AlexaForBusinessReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AlexaForBusinessReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:47 UTC
- Ora modificata: 20 novembre 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAPIGatewayAdministrator

Descrizione: fornisce l'accesso completo create/edit/delete APIs ad Amazon API Gateway tramite Console di gestione AWS.

`AmazonAPIGatewayAdministrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAPIGatewayAdministrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:34 UTC
- Ora modificata: 9 luglio 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:*"
      ],
```

```
      "Resource" : "arn:aws:apigateway:*::/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAPIGatewayInvokeFullAccess

Descrizione: fornisce l'accesso completo per richiamare APIs in Amazon API Gateway.

`AmazonAPIGatewayInvokeFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAPIGatewayInvokeFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:36 UTC
- Ora modificata: 18 dicembre 2018, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : "arn:aws:execute-api:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAPIGatewayPushToCloudWatchLogs

Descrizione: consente ad API Gateway di inviare i log all'account dell'utente.

`AmazonAPIGatewayPushToCloudWatchLogs`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAPIGatewayPushToCloudWatchLogs` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 novembre 2015, 23:41 UTC

- Ora modificata: 11 novembre 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAppFlowFullAccess

Descrizione: fornisce l'accesso completo ad Amazon AppFlow e l'accesso ai AWS servizi supportati come origine o destinazione del flusso (S3 e Redshift). Fornisce inoltre l'accesso a KMS per la crittografia

`AmazonAppFlowFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAppFlowFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 giugno 2020, 23:30 UTC
- Ora modificata: 28 febbraio 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appflow:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesForRedshift",
      "Effect" : "Allow",
```

```
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSListGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3ReadAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3PutBucketPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::appflow-*"
    },
    {
      "Sid" : "SecretsManagerCreateSecretAccess",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
```

```
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "LambdaListFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAppFlowReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ai flussi di Amazon Appflow

`AmazonAppFlowReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAppFlowReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 giugno 2020, 23:26 UTC

- Ora modificata: 28 febbraio 2022, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnector",
        "appflow:DescribeConnectors",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlows",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListConnectorFields",
        "appflow:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

Descrizione: concede le autorizzazioni ad ARC Region Switch per l'esecuzione e la valutazione del piano.

`AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 novembre 2025, 19:34 UTC
- Ora modificata: 5 marzo 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "arc-region-switch:GetPlan",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:ListPlanExecutions"
      ],
      "Resource" : "*",
      "Sid" : "GetPlanAndExecutions"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:SimulatePrincipalPolicy",
      "Resource" : "arn:aws:iam::*:role/*",
      "Sid" : "PlanEvaluation"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*",
      "Sid" : "CloudWatch"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAppStreamFullAccess

Descrizione: fornisce l'accesso completo ad Amazon AppStream tramite Console di gestione AWS.

`AmazonAppStreamFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAppStreamFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 28 agosto 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "appstream:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
```

```
        "application-autoscaling:DeleteScheduledAction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:ListRoles",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
ApplicationAutoScalingForAmazonAppStreamAccess",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appstream.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_AppStreamFleet",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "appstream.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAppStreamPCAAccess

Descrizione: accesso Amazon AppStream 2.0 alla CA privata di AWS Certificate Manager negli account dei clienti per l'autenticazione basata su certificati

`AmazonAppStreamPCAAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonAppStreamPCAAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 ottobre 2022, 17:05 UTC
- Ora modificata: 24 ottobre 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAppStreamReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon AppStream tramite Console di gestione AWS.

`AmazonAppStreamReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAppStreamReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:List*",
        "appstream:Describe*"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAppStreamServiceAccess

Descrizione: politica predefinita per il ruolo AppStream di servizio Amazon.

`AmazonAppStreamServiceAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAppStreamServiceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 novembre 2016, 04:17 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::appstream2-36fb080bb8-*",
        "arn:aws:s3:::appstream-app-settings-*",
        "arn:aws:s3:::appstream-logs-*"
```

```
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAthenaFullAccess

Descrizione: Fornisci accesso completo ad Amazon Athena e accesso mirato alle dipendenze necessarie per consentire l'esecuzione di query, la scrittura dei risultati e la gestione dei dati.

`AmazonAthenaFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonAthenaFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2016, 16:46 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:StartColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
```

```
        "glue:GetCatalogImportStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseQueryResultsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Sid" : "BaseAthenaExamplesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::athena-examples*"
      ]
    },
    {
      "Sid" : "BaseS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "BaseSNSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseCloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseDataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListDomains",
        "datazone:ListProjects",
        "datazone:ListAccountEnvironments"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BasePricingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAthenaServiceRolePolicy

Descrizione: consente l'accesso ad altre risorse di AWS servizio necessarie per eseguire Amazon Athena

`AmazonAthenaServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 14 novembre 2025, 22:34 UTC
- Ora modificata: 14 novembre 2025, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonAthenaServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Athena",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAugmentedAIFullAccess

Descrizione: fornisce l'accesso per eseguire tutte le operazioni, le risorse Amazon Augmented AI HumanTaskUis , FlowDefinitions HumanLoops tra cui e. Non consente l'accesso per creare FlowDefinitions contro il pubblico Workteam.

`AmazonAugmentedAIFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonAugmentedAIFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 16:21 UTC
- Ora modificata: 03 dicembre 2019, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAugmentedAIHumanLoopFullAccess

Descrizione: fornisce l'accesso per eseguire tutte le operazioni su HumanLoops.

`AmazonAugmentedAIHumanLoopFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAugmentedAIHumanLoopFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 16:20 UTC
- Ora modificata: 03 dicembre 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAugmentedAIIntegratedAPIAccess

Descrizione: fornisce l'accesso per eseguire tutte le operazioni, le risorse Amazon Augmented AI HumanTaskUis , FlowDefinitions HumanLoops tra cui e. Fornisce inoltre l'accesso a quelle operazioni dei servizi integrati con Amazon Augmented AI.

`AmazonAugmentedAIIntegratedAPIAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAugmentedAIIntegratedAPIAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 aprile 2020, 20:47 UTC
- Ora modificata: 22 aprile 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectModerationLabels"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAuroraDSQLConsoleFullAccess

Descrizione: Fornisce l'accesso amministrativo completo da console ad Aurora DSQL

`AmazonAuroraDSQLConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAuroraDSQLConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 dicembre 2024, 15:36 UTC
- Ora modificata: 13 maggio 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLConsoleFullAccess`

Versione della politica

Versione della politica: v16 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError",
        "dsql:CreateStream",
```

```
        "dsql:DeleteStream",
        "dsql:GetStream",
        "dsql:ListStreams",
        "dsql:UpdateStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DsqlConsolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ValidatePolicy",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "kms:DescribeKey",
        "cloudwatch:ListMetrics",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
```

```
      }
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRoleForChangeStreams",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "dsql.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAuroraDSQLFullAccess

Descrizione: Fornisce accesso amministrativo completo a Aurora DSQL

`AmazonAuroraDSQLFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAuroraDSQLFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 dicembre 2024, 15:36 UTC
- Ora modificata: 13 maggio 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLFullAccess`

Versione della politica

Versione della politica: v16 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
```

```
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError",
        "dsql:CreateStream",
        "dsql:DeleteStream",
        "dsql:GetStream",
        "dsql:ListStreams",
        "dsql:UpdateStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSDescribePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForChangeStreams",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonAuroraDSQLReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Aurora DSQL

`AmazonAuroraDSQLReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonAuroraDSQLReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 dicembre 2024, 15:21 UTC
- Ora modificata: 13 maggio 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLReadOnlyAccess`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetClusterPolicy",
        "dsql:GetCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dsql:GetStream",
        "dsql:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRo

Descrizione: fornisce l'autorizzazione di inferenza del modello Bedrock alla memoria principale dell'agente Bedrock

`AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy`è una policy gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 luglio 2025, 13:37 UTC
- Ora modificata: 17 luglio 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy`

Versione della politica

Versione della politica: v4 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockInvokeModel",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockMantleInference",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CreateInference",
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CallWithBearerToken",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockExternalWebSearchFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Bedrock Web Search, incluso il recupero di contenuti da siti Web esterni al di fuori dei confini della AWS rete.

`AmazonBedrockExternalWebSearchFullAccess`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockExternalWebSearchFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 agosto 2026, 16:57 UTC
- Ora modificata: 3 agosto 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockExternalWebSearchFullAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockExternalWebSearchFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch",
```

```
        "bedrock-websearch:ExternalWebAccess"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockExternalWebSearchReadOnly

Descrizione: fornisce l'accesso in sola lettura ad Amazon Bedrock Web Search, incluso il recupero di contenuti da siti Web esterni al di fuori dei confini della rete. AWS

`AmazonBedrockExternalWebSearchReadOnly`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockExternalWebSearchReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 agosto 2026, 16:57 UTC
- Ora modificata: 3 agosto 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockExternalWebSearchReadOnly`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockExternalWebSearchReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch",
        "bedrock-websearch:ExternalWebAccess"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockFullAccess

Descrizione: fornisce un accesso completo ad Amazon Bedrock e un accesso limitato ai servizi correlati da esso richiesti

`AmazonBedrockFullAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 06 dicembre 2023, 15:47 UTC
- Ora modificata: 4 agosto 2026, 05:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Versione della politica

Versione della politica: v11 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
```

```
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
```

```
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointAddTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:RequestTag/bedrock:marketplace-registration-status" : "registered",
          "aws:RequestTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointDeleteTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
```

```
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:ResourceTag/bedrock:marketplace-registration-status" : "registered",
          "aws:ResourceTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointInvokingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    },
    {
      "Sid" : "PassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*ForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "PassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockLimitedAccess

Descrizione: fornisce un accesso limitato ad Amazon Bedrock e ai servizi correlati da esso richiesti

`AmazonBedrockLimitedAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockLimitedAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 giugno 2025, 22:22 UTC
- Ora modificata: 4 agosto 2026, 05:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess`

Versione della politica

Versione della politica: v9 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*",
        "bedrock:CallWithBearerToken",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CancelAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:CreateAutomatedReasoningPolicy",
```

```
        "bedrock:CreateAutomatedReasoningPolicyTestCase",
        "bedrock:CreateAutomatedReasoningPolicyVersion",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreateGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreateInferenceProfile",
        "bedrock:CreateModelCopyJob",
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateModelImportJob",
        "bedrock:CreateModelInvocationJob",
        "bedrock:CreatePromptRouter",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:DeleteAutomatedReasoningPolicy",
        "bedrock:DeleteAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:DeleteAutomatedReasoningPolicyTestCase",
        "bedrock:DeleteCustomModel",
        "bedrock:DeleteGuardrail",
        "bedrock:DeleteImportedModel",
        "bedrock:DeleteInferenceProfile",
        "bedrock:DeletePromptRouter",
        "bedrock:DeleteProvisionedModelThroughput",
        "bedrock:ExportAutomatedReasoningPolicyVersion",
        "bedrock:StartAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:StartAutomatedReasoningPolicyTestWorkflow",
        "bedrock:StopEvaluationJob",
        "bedrock:StopModelCustomizationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:TagResource",
        "bedrock:UntagResource",
        "bedrock:UpdateAutomatedReasoningPolicy",
        "bedrock:UpdateAutomatedReasoningPolicyAnnotations",
        "bedrock:UpdateAutomatedReasoningPolicyTestCase",
        "bedrock:UpdateGuardrail",
        "bedrock:UpdateProvisionedModelThroughput",
        "bedrock:ApplyGuardrail",
        "bedrock:InvokeAutomatedReasoningPolicy",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "bedrock.amazonaws.com",
            "bedrock-mantle.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockMantleFullAccess

Descrizione: fornisce un accesso completo ad Amazon Bedrock Mantle e un accesso limitato ai servizi correlati da esso richiesti

`AmazonBedrockMantleFullAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockMantleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 dicembre 2025, 07:19 UTC
- Ora modificata: 4 agosto 2026, 04:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleFullAccess`

Versione della politica

Versione della politica: v5 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockMantleFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-mantle.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockMantleInferenceAccess

Descrizione: fornisce l'accesso in lettura e creazione di inferenze ad Amazon Bedrock Mantle

`AmazonBedrockMantleInferenceAccess`è una policy gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockMantleInferenceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 dicembre 2025, 07:19 UTC
- Ora modificata: 4 agosto 2026, 05:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleInferenceAccess`

Versione della politica

Versione della politica: v5 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleInference",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockMantleFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-mantle.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockMantleReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon Bedrock Mantle

`AmazonBedrockMantleReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockMantleReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 dicembre 2025, 07:19 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*"
      ],
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*"
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockMarketplaceAccess

Descrizione: Fornisce un accesso limitato ad Amazon Bedrock Marketplace e ai servizi correlati da esso richiesti

`AmazonBedrockMarketplaceAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockMarketplaceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 giugno 2025, 22:22 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMarketplaceAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMarketplaceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateMarketplaceModelEndpoint",
        "bedrock:DeleteMarketplaceModelEndpoint",
        "bedrock:DeregisterMarketplaceModelEndpoint",
        "bedrock:RegisterMarketplaceModelEndpoint",
        "bedrock:UpdateMarketplaceModelEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointAddTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:RequestTag/bedrock:marketplace-registration-status" : "registered",
          "aws:RequestTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
```

```
    },
    {
      "Sid" : "MarketplaceModelEndpointDeleteTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:ResourceTag/bedrock:marketplace-registration-status" : "registered",
          "aws:ResourceTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointInvokingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    },
    {
      "Sid" : "PassRoleToSageMaker",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*ForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockReadOnly

Descrizione: Fornisce accesso in sola lettura ad Amazon Bedrock

`AmazonBedrockReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 dicembre 2023, 15:48 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockStudioPermissionsBoundary

Descrizione: definisce le autorizzazioni massime dei ruoli IAM che Amazon Bedrock Studio crea per gestire le risorse di Amazon Bedrock Studio.

`AmazonBedrockStudioPermissionsBoundary`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockStudioPermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 agosto 2024, 00:24 UTC
- Ora modificata: 01 agosto 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockStudioPermissionsBoundary`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::br-studio-${aws:PrincipalAccount}-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessOpenSearchCollections",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*::foundation-model/*"
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
```

```
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:ListTagsForResource",
        "bedrock:TagResource",
        "bedrock:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RetrieveAndGenerate",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "WriteLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/br-studio-*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "InvokeLambdaFunctions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:br-studio-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretsManagerSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:br-studio/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "UseKmsKeyWithBedrock",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/EnableBedrock" : "true"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "UseKmsKeyWithAwsServices",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/EnableBedrock" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockWebSearchFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Bedrock Web Search. I dati rimangono all'interno dei confini AWS della rete.

`AmazonBedrockWebSearchFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockWebSearchFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 agosto 2026, 16:42 UTC
- Ora modificata: 3 agosto 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockWebSearchFullAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockWebSearchFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBedrockWebSearchReadOnly

Descrizione: fornisce l'accesso in sola lettura ad Amazon Bedrock Web Search. I dati rimangono all'interno dei confini della rete. AWS

`AmazonBedrockWebSearchReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonBedrockWebSearchReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 agosto 2026, 16:57 UTC
- Ora modificata: 3 agosto 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockWebSearchReadOnly`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockWebSearchReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBraketFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Braket tramite l'SDK Console di gestione AWS and. Fornisce inoltre l'accesso ai servizi correlati (ad esempio, S3, log).

`AmazonBraketFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonBraketFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 agosto 2020, 20:12 UTC
- Ora modificata: 6 luglio 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AmazonBraket" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "servicequotas:GetServiceQuota",
        "cloudwatch:GetMetricData",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListNotebookInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
```

```
        "sagemaker:ListTags",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/amazon-
braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "braket:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/braket.amazonaws.com/
AWSServiceRoleForAmazonBraket*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "braket.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonBraketServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
```

```
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
```

```
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBraketJobsExecutionPolicy

Descrizione: concede l'accesso Servizi AWS e le risorse necessarie per l'esecuzione di un Amazon Braket Job tra cui S3, Cloudwatch, IAM e Braket

`AmazonBraketJobsExecutionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonBraketJobsExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 novembre 2021, 19:34 UTC
- Ora modificata: 6 luglio 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AmazonBraket" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "braket:CancelJob",
        "braket:CancelQuantumTask",
        "braket:CreateJob",
        "braket:CreateQuantumTask",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "braket:ListTagsForResource",
        "braket:TagResource",
        "braket:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonBraketServiceRolePolicy

Descrizione: Consente ad Amazon Braket di creare e gestire AWS risorse per tuo conto

`AmazonBraketServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 04 agosto 2020, 17:12 UTC
- Ora modificata: 6 luglio 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AmazonBraket" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonChimeFullAccess

Descrizione: fornisce l'accesso completo alla Console di amministrazione di Amazon Chime tramite. Console di gestione AWS

`AmazonChimeFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonChimeFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 novembre 2017, 22:15 UTC
- Ora modificata: 14 dicembre 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "chime:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Action" : [
        "kinesis:ListStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-chat-*",
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::chime-chat-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonChimeReadOnly

Descrizione: fornisce l'accesso in sola lettura alla Console di amministrazione di Amazon Chime tramite. Console di gestione AWS

`AmazonChimeReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonChimeReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 novembre 2017, 22:04 UTC
- Ora modificata: 14 dicembre 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:List*",
        "chime:Get*",
        "chime:Describe*",
        "chime:SearchAvailablePhoneNumbers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonChimeSDK

Descrizione: Fornisce l'accesso alle operazioni dell'SDK Amazon Chime

`AmazonChimeSDK`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonChimeSDK` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 febbraio 2020, 21:53 UTC
- Ora modificata: 10 gennaio 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMeeting",
        "chime:CreateMeetingWithAttendees",
        "chime:DeleteMeeting",
        "chime:GetMeeting",
        "chime:ListMeetings",
        "chime:CreateAttendee",
        "chime:BatchCreateAttendee",
        "chime:DeleteAttendee",
        "chime:GetAttendee",
        "chime:ListAttendees",
        "chime:ListAttendeeTags",
        "chime:ListMeetingTags",
        "chime:ListTagsForResource",
        "chime:TagAttendee",
        "chime:TagMeeting",
        "chime:TagResource",
        "chime:UntagAttendee",
        "chime:UntagMeeting",
        "chime:UntagResource",
        "chime:StartMeetingTranscription",
        "chime:StopMeetingTranscription",
        "chime:CreateMediaCapturePipeline",
        "chime:CreateMediaConcatenationPipeline",
        "chime:CreateMediaLiveConnectorPipeline",
        "chime:DeleteMediaCapturePipeline",
        "chime:DeleteMediaPipeline",
        "chime:GetMediaCapturePipeline",
```

```
        "chime:GetMediaPipeline",
        "chime:ListMediaCapturePipelines",
        "chime:ListMediaPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Descrizione: Policy gestita per il ruolo collegato al servizio Amazon Chime SDK MediaPipelines

`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 4 aprile 2022, 22:02 UTC
- Ora modificata: 08 dicembre 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricsForChimeSDKNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ChimeSDK"
        }
      }
    },
    {
      "Sid" : "AllowKinesisVideoStreamsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeMediaPipelines-*"
      ]
    },
    {
      "Sid" : "AllowKinesisVideoStreamsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "AllowChimeMeetingAccess",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMeeting",
        "chime:CreateAttendee",
        "chime:DeleteAttendee"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonChimeSDKMessagingServiceRolePolicy

Descrizione: consente ad Amazon Chime SDK Messaging di accedere alle AWS risorse e abilitare la funzionalità di messaggistica

`AmazonChimeSDKMessagingServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 03 marzo 2023, 01:43 UTC
- Ora modificata: 03 marzo 2023, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "kinesis.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonChimeServiceRolePolicy

Descrizione: consente l'accesso alle AWS risorse utilizzate o gestite da Amazon Chime

`AmazonChimeServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 30 settembre 2019, 22:25 UTC
- Ora modificata: 30 settembre 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/
AWSServiceRoleForAmazonChime"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "chime.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonChimeTranscriptionServiceLinkedRolePolicy

Descrizione: consente ad Amazon Chime di accedere ad Amazon Transcribe e Amazon Transcribe Medical per tuo conto

`AmazonChimeTranscriptionServiceLinkedRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 4 agosto 2021, 21:47 UTC
- Ora modificata: 04 agosto 2021, 21:47 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:StartStreamTranscription",
        "transcribe:StartMedicalStreamTranscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonChimeUserManagement

Descrizione: fornisce l'accesso alla gestione degli utenti alla Console di amministrazione di Amazon Chime tramite. Console di gestione AWS

`AmazonChimeUserManagement`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonChimeUserManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 novembre 2017, 22:17 UTC
- Ora modificata: 18 febbraio 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:ListAccounts",
        "chime:GetAccount",
        "chime:GetAccountSettings",
        "chime:UpdateAccountSettings",
        "chime:ListUsers",
        "chime:GetUser",
        "chime:GetUserByEmail",
        "chime:InviteUsers",
        "chime:InviteUsersFromProvider",
        "chime:SuspendUsers",
        "chime:ActivateUsers",
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
```

```
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime:ListGroups",
        "chime:SubmitSupportRequest",
        "chime:ListDelegates",
        "chime:ListAccountUsageReportData",
        "chime:GetMeetingDetail",
        "chime:ListMeetingEvents",
        "chime:ListMeetingsReportData",
        "chime:GetUserActivityReportData",
        "chime:UpdateUser",
        "chime:BatchUpdateUser",
        "chime:BatchSuspendUser",
        "chime:BatchUnsuspendUser",
        "chime:AssociatePhoneNumberWithUser",
        "chime:DisassociatePhoneNumberFromUser",
        "chime:GetPhoneNumber",
        "chime:ListPhoneNumbers",
        "chime:GetUserSettings",
        "chime:UpdateUserSettings",
        "chime:CreateUser",
        "chime:AssociateSigninDelegateGroupsWithAccount",
        "chime:DisassociateSigninDelegateGroupsFromAccount"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Descrizione: policy gestita per Service Linked Role per Amazon Chime VoiceConnector

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 30 settembre 2019, 22:16 UTC
- Ora modificata: 14 aprile 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeVoiceConnector-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMediaInsightsPipeline",
        "chime:GetMediaInsightsPipelineConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCloudDirectoryFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Cloud Directory Service.

`AmazonCloudDirectoryFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCloudDirectoryFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 febbraio 2017, 00:41 UTC
- Ora modificata: 25 febbraio 2017, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "clouddirectory:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCloudDirectoryReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Cloud Directory Service.

`AmazonCloudDirectoryReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCloudDirectoryReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 febbraio 2017, 23:42 UTC
- Ora modificata: 28 febbraio 2017, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "clouddirectory:List*",
        "clouddirectory:Get*",
        "clouddirectory:LookupPolicy",
        "clouddirectory:BatchRead"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCloudWatchEvidentlyFullAccess

Descrizione: fornisce solo l'accesso completo ad Amazon CloudWatch Evidently. Fornisce inoltre l'accesso ad Amazon S3, Amazon SNS, CloudWatch Amazon e altri servizi correlati.

`AmazonCloudWatchEvidentlyFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCloudWatchEvidentlyFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 15:10 UTC
- Ora modificata: 29 novembre 2021, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchRUMEvidentlyRole-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:TagResource",
        "cloudwatch:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Evidently-Alarm-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Evidently-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCloudWatchEvidentlyReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon CloudWatch Evidently

`AmazonCloudWatchEvidentlyReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCloudWatchEvidentlyReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 15:08 UTC
- Ora modificata: 29 novembre 2021, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCloudWatchEvidentlyServiceRolePolicy

Descrizione: consente a CloudWatch Evidently Service di gestire AWS le risorse associate per conto del cliente

`AmazonCloudWatchEvidentlyServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 13 settembre 2022, 17:25 UTC
- Ora modificata: 13 settembre 2022, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StartDeployment",
      "Resource" : [
        "arn:aws:appconfig:*:*:application/*",
        "arn:aws:appconfig:*:*:deploymentstrategy/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StartDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/configurationprofile/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/Owner" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:TagResource",
      "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StopDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StopDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:ListDeployments",
```

```
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCloudWatchRUMFullAccess

Descrizione: concede le autorizzazioni di accesso complete per il servizio Amazon RUM CloudWatch

`AmazonCloudWatchRUMFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCloudWatchRUMFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 15:46 UTC
- Ora modificata: 29 novembre 2021, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/rum.amazonaws.com/
AWSServiceRoleForRealUserMonitoring"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/RUM-Monitor*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles"
      ],
      "Resource" : "arn:aws:cognito-identity:*:*:identitypool/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*RUMService*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCloudWatchRUMReadOnlyAccess

Descrizione: concede autorizzazioni di sola lettura per il servizio Amazon RUM CloudWatch

`AmazonCloudWatchRUMReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCloudWatchRUMReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 15:43 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListRumMetricsDestinations",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetResourcePolicy",
        "rum:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanariesLastRun",
        "synthetics:describeCanaries"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCloudWatchRUMServiceRolePolicy

Descrizione: concede l'autorizzazione ad Amazon CloudWatch RUM Service per pubblicare dati di monitoraggio su altri servizi pertinenti AWS

`AmazonCloudWatchRUMServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 novembre 2021, 23:17 UTC
- Ora modificata: 22 febbraio 2023, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "RUM/CustomMetrics/*",
            "AWS/RUM"
```

```
            ]
          }
        }
      }
    ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeCatalystFullAccess

Descrizione: Fornisce accesso completo ad Amazon CodeCatalyst

`AmazonCodeCatalystFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCodeCatalystFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 aprile 2023, 16:50 UTC
- Ora modificata: 20 aprile 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCatalystResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:*",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCatalystAssociateIAMRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codecatalyst.amazonaws.com",
            "codecatalyst-runner.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeCatalystReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon CodeCatalyst

`AmazonCodeCatalystReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCodeCatalystReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 aprile 2023, 16:49 UTC
- Ora modificata: 20 aprile 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:Get*",
        "codecatalyst:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeCatalystSupportAccess

Descrizione: consente CodeCatalyst ad Amazon di creare, aggiornare e risolvere Supporto AWS casi per tuo conto.

`AmazonCodeCatalystSupportAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCodeCatalystSupportAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2023, 12:34 UTC
- Ora modificata: 20 aprile 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportLevel",
        "support:SearchForCases",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:InitiateCallForCase",
        "support:InitiateChatForCase",
        "support:PutCaseAttributes",
        "support:RateCaseCommunication",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeGuruProfilerAgentAccess

Descrizione: fornisce l'accesso richiesto dall'agente Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerAgentAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCodeGuruProfilerAgentAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 febbraio 2021, 22:11 UTC
- Ora modificata: 5 maggio 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ConfigureAgent",
        "codeguru-profiler:CreateProfilingGroup",
        "codeguru-profiler:PostAgentProfile"
      ],
      "Resource" : "arn:aws:codeguru-profiler:*:*:profilingGroup/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeGuruProfilerFullAccess

Descrizione: fornisce l'accesso completo ad Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCodeGuruProfilerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 10:13 UTC
- Ora modificata: 15 luglio 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru-profiler:*",
```

```
        "iam:ListRoles",
        "iam:ListUsers",
        "sns:ListTopics",
        "codeguru:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/*AWSServiceRoleForCodeGuruProfiler*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "codeguru-profiler.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeGuruProfilerReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCodeGuruProfilerReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 dicembre 2019, 10:30 UTC
- Ora modificata: 27 giugno 2020, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru:Get*",
        "codeguru-profiler:BatchGet*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeGuruReviewerFullAccess

Descrizione: concede l'accesso completo ad Amazon CodeGuru Reviewer e l'accesso mirato alle dipendenze richieste.

`AmazonCodeGuruReviewerFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonCodeGuruReviewerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 08:33 UTC
- Ora modificata: 29 agosto 2020, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codeguru-reviewer:*",
        "codeguru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer"
    },
    {
      "Sid" : "CodeCommitAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:TagResource",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:PassConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListRepositories",
            "ListOwners"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
```

```
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeGuruReviewerReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon CodeGuru Reviewer.

`AmazonCodeGuruReviewerReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCodeGuruReviewerReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 08:48 UTC
- Ora modificata: 29 agosto 2020, 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru:Get*",
        "codeguru-reviewer:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeGuruReviewerServiceRolePolicy

Descrizione: un ruolo collegato al servizio richiesto ad Amazon CodeGuru Reviewer per accedere alle risorse per tuo conto.

`AmazonCodeGuruReviewerServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 03 dicembre 2019, 05:31 UTC
- Ora modificata: 27 novembre 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCodeGuruReviewerEnabledRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetRepository",
        "codecommit:GetBranch",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetDifferences",
        "codecommit:GetPullRequest",
        "codecommit:ListPullRequests",
        "codecommit:PostCommentForPullRequest",
```

```
        "codecommit:GitPull",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/codeguru-reviewer" : "enabled"
        }
      }
    },
    {
      "Sid" : "AccessCodeGuruReviewerEnabledConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListBranches",
            "GetBranch",
            "ListRepositories",
            "ListOwners",
            "ListPullRequests",
            "GetPullRequest",
            "ListPullRequestComments",
            "ListPullRequestCommits",
            "ListCommitFiles",
            "ListBranchCommits",
            "CreatePullRequestDiffComment",
            "GitPull"
          ]
        },
        "Null" : {
          "aws:ResourceTag/codeguru-reviewer" : "false"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsResourceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
```

```
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGuruS3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::codeguru-reviewer-*",
        "arn:aws:s3:::codeguru-reviewer-*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeGuruSecurityFullAccess

Descrizione: fornisce l'accesso completo ad Amazon CodeGuru Security.

`AmazonCodeGuruSecurityFullAccess` è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCodeGuruSecurityFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 09 maggio 2023, 21:03 UTC
- Ora modificata: 09 maggio 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCodeGuruSecurityScanAccess

Descrizione: fornisce l'accesso necessario per lavorare con le scansioni CodeGuru di Amazon Security.

`AmazonCodeGuruSecurityScanAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCodeGuruSecurityScanAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 maggio 2023, 20:54 UTC
- Ora modificata: 09 maggio 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityScanAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:CreateUploadUrl",
        "codeguru-security:GetScan",
        "codeguru-security:GetFindings"
```

```
      ],
      "Resource" : "arn:aws:codeguru-security:*:*:scans/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCognitoDeveloperAuthenticatedIdentities

Descrizione: fornisce l'accesso ad Amazon Cognito per APIs supportare le identità autenticate degli sviluppatori dal tuo backend di autenticazione.

`AmazonCognitoDeveloperAuthenticatedIdentities`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonCognitoDeveloperAuthenticatedIdentities` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 marzo 2015, 17:22 UTC
- Ora modificata: 24 marzo 2015, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:MergeDeveloperIdentities",
        "cognito-identity:UnlinkDeveloperIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCognitoIdpEmailServiceRolePolicy

Descrizione: consente al servizio Amazon Cognito User Pools di utilizzare le identità SES per l'invio di e-mail

`AmazonCognitoIdpEmailServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 marzo 2019, 21:32 UTC
- Ora modificata: 21 marzo 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ses:List*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCognitoIdpServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite dai pool di utenti di Amazon Cognito

`AmazonCognitoIdpServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 giugno 2020, 22:30 UTC
- Ora modificata: 26 giugno 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCognitoPowerUser

Descrizione: fornisce l'accesso amministrativo alle risorse Amazon Cognito esistenti. Avrai bisogno dei privilegi di Account AWS amministratore per creare nuove risorse Cognito.

`AmazonCognitoPowerUser`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCognitoPowerUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 marzo 2015, 17:14 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "iam:ListRoles",
        "iam:ListOpenIdConnectProviders",
        "iam:GetRole",
        "iam:ListSAMLProviders",
        "iam:GetSAMLProvider",
        "kinesis:ListStreams",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "sns:GetSMSSandboxAccountStatus",
        "sns:ListPlatformApplications",
        "ses:ListIdentities",
        "ses:GetIdentityVerificationAttributes",
        "mobiletargeting:GetApps",
        "acm:ListCertificates",
        "sms-voice:DescribeAccountAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : [
            "cognito-idp.amazonaws.com",
            "email.cognito-idp.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdp*",
        "arn:aws:iam::*:role/aws-service-role/email.cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdpEmail*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCognitoReadOnly

Descrizione: fornisce accesso in sola lettura alle risorse di Amazon Cognito.

`AmazonCognitoReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonCognitoReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 marzo 2015, 17:06 UTC
- Ora modificata: 01 agosto 2019, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:Describe*",
        "cognito-identity:Get*",
        "cognito-identity:List*",
        "cognito-idp:Describe*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:List*",
        "cognito-idp:Get*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "iam:ListOpenIdConnectProviders",
        "iam:ListRoles",
        "sns:ListPlatformApplications"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCognitoUnAuthedIdentitiesSessionPolicy

Descrizione: questa politica definisce l'insieme di autorizzazioni consentite per le identità non autenticate per i pool di identità di Cognito. Questa politica non è pensata per essere utilizzata come politica di autorizzazione autonoma. Viene utilizzata come barriera contro le politiche eccessivamente permissive relative ai ruoli in un pool di identità. Non associate questa policy a nessun ruolo, poiché Cognito Identity Service la includerà automaticamente come policy ristretta al momento della creazione delle credenziali. I privilegi per accedere temporaneamente ad altre AWS risorse tramite il flusso avanzato saranno ora definiti dall'intersezione tra il ruolo associato all'identità dell'utente non autenticato fornito da un servizio e i privilegi concessi in questa politica gestita di proprietà di Cognito.

`AmazonCognitoUnAuthedIdentitiesSessionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonCognitoUnAuthedIdentitiesSessionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 luglio 2023, 23:04 UTC
- Ora modificata: 01 maggio 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CognitoUnAuthedIdentitiesSessionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "rum:PutRumEvents",
        "sagemaker:InvokeEndpoint",
        "polly:*",
        "comprehend:*",
        "translate:*",
        "transcribe:*",
        "rekognition:*",
        "mobiletargeting:*",
        "firehose:*",
        "personalize:*",
        "geo:GetMap*",
        "geo:ListMaps",
        "geo:SearchPlaceIndex*",
        "geo:GetPlace",
        "geo:CalculateRoute*",
        "geo:*Geofence",
        "geo:*Geofences",
        "geo:*DevicePosition*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyPair",
        "kms:GenerateDataKeyPairWithoutPlaintext",
        "kms:GenerateDataKeyWithoutPlaintext"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonCognitoUnauthenticatedIdentities

Descrizione: questa politica definisce l'insieme di autorizzazioni consentite per le identità non autenticate per i pool di identità di Cognito. Non è necessario che questo sia associato al ruolo unauth, poiché Cognito Identity Service lo includerà automaticamente come policy ristretta durante la creazione delle credenziali. I privilegi per accedere temporaneamente ad altre AWS risorse tramite il flusso avanzato saranno ora definiti dall'intersezione tra il ruolo associato all'identità dell'utente non autenticato fornito da un servizio e i privilegi concessi in questa politica gestita di proprietà di Cognito.

`AmazonCognitoUnauthenticatedIdentities`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonCognitoUnauthenticatedIdentities` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 febbraio 2023, 22:36 UTC
- Ora modificata: 01 febbraio 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "rum:PutRumEvents",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonConnect_FullAccess

Descrizione: lo scopo di questa politica è concedere le autorizzazioni agli utenti AWS Connect necessari per utilizzare le risorse Connect. Questa politica fornisce l'accesso completo alle risorse AWS Connect tramite Connect Console e pubbliche. APIs

`AmazonConnect_FullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonConnect_FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2020, 19:54 UTC
- Ora modificata: 07 marzo 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:*",
        "ds:CreateAlias",
        "ds:AuthorizeApplication",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:UnauthorizeApplication",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lex:GetBots",
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:CreateLogGroup",
```

```
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "lambda:ListFunctions",
        "ds:CheckAlias",
        "profile:ListAccountIntegrations",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:GetProfileObjectType",
        "profile:ListProfileObjectTypeTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "profile:AddProfileKey",
        "profile:CreateDomain",
        "profile:CreateProfile",
        "profile:DeleteDomain",
        "profile:DeleteIntegration",
        "profile:DeleteProfile",
        "profile:DeleteProfileKey",
        "profile:DeleteProfileObject",
        "profile:DeleteProfileObjectType",
        "profile:GetIntegration",
        "profile:GetMatches",
        "profile:GetProfileObjectType",
        "profile:ListIntegrations",
        "profile:ListProfileObjects",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "profile:MergeProfiles",
        "profile:PutIntegration",
        "profile:PutProfileObject",
        "profile:PutProfileObjectType",
        "profile:SearchProfiles",
        "profile:TagResource",
        "profile:UntagResource",
        "profile:UpdateDomain",
        "profile:UpdateProfile"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:connect/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "connect.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:DeleteServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "profile.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonConnectCampaignsServiceLinkedRolePolicy

Descrizione: Policy per il ruolo collegato al servizio Amazon Connect Campaigns

`AmazonConnectCampaignsServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 23 settembre 2021, 20:54 UTC
- Ora modificata: 18 giugno 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConnectCampaignAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:ListCampaigns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectCampaignsMetricsAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:GetMetricDataV2"
      ],
      "Resource" : "arn:aws:connect-campaigns:*:*:campaign/*"
    },
    {
      "Sid" : "ConnectAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:BatchPutContact",
        "connect:StopContact",
        "connect:DescribeContactFlow",
        "connect:SendOutboundEmail",
        "connect:SendOutboundWebNotification"
      ],
      "Resource" : "arn:aws:connect:*:*:instance/*"
    },
    {
      "Sid" : "ConnectChatAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:SendOutboundChatMessage"
      ],
      "Resource" : [
        "arn:aws:connect:*:*:instance/*",
        "arn:aws:connect:*:*:phone-number/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AllowSocialMessagingSendMessageOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:SendWhatsAppMessage"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:phone-number-id/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSocialMessagingTemplateOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:GetWhatsAppMessageTemplate"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:waba/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeListRuleAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeManagedResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "connect-campaigns.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTargetsByRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectCampaignsEnabledTaggedResources",
      "Effect" : "Allow",
```

```
      "Action" : [
        "wisdom:GetMessageTemplate",
        "wisdom:RenderMessageTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectCampaignsEnabled" : "True"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonConnectReadOnlyAccess

Descrizione: concede l'autorizzazione a visualizzare le istanze Amazon Connect nel tuo. Account AWS

`AmazonConnectReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonConnectReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 ottobre 2018, 21:00 UTC
- Ora modificata: 19 giugno 2024, 15:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "connect:Get*",
        "connect:Describe*",
        "connect:List*",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyConnectEmergencyAccess",
      "Effect" : "Deny",
      "Action" : "connect:AdminGetEmergencyAccessToken",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonConnectServiceLinkedRolePolicy

Descrizione: consente ad Amazon Connect di creare e gestire AWS risorse per tuo conto.

`AmazonConnectServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 07 settembre 2018, 00:21 UTC
- Ora modificata: 27 maggio 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v55 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:*"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "AllowDeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect_*"
    },
    {
      "Sid" : "AllowS3ObjectForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*/*"
      ]
    },
    {
      "Sid" : "AllowGetBucketMetadataForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*"
      ]
    },
    {
      "Sid" : "AllowConnectLogGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/connect/*:*"
      ]
    },
    {
      "Sid" : "AllowListLexBotAccess",
      "Effect" : "Allow",
      "Action" : [
        "lex:ListBots",
        "lex:ListBotAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesForConnectDomain",
      "Effect" : "Allow",
      "Action" : "profile:*",
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*",
        "arn:aws:profile:*:*:/domains/amazon-connect-*",
        "arn:aws:profile:*:*:/templates*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowCustomerProfilesListOperations",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListRecommenderRecipes",
        "profile:ListAccountIntegrations",
        "profile:ListDomains"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "DenyCustomerProfilesForConnectDomain",
      "Effect" : "Deny",
      "Action" : [
        "profile:CreateDomain",
        "profile:UpdateDomain",
        "profile:DeleteDomain",
        "profile:CreateEventStream",
        "profile:DeleteEventStream",
        "profile:DeleteWorkflow",
        "profile:DeleteProfileKey",
        "profile:UntagResource",
        "profile:TagResource",
        "profile:CreateIntegrationWorkflow"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/*"
    },
    {
      "Sid" : "AllowAppIntegrationsForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "app-integrations:GetDataIntegration",
        "app-integrations:ListDataIntegrationAssociations",
        "app-integrations:CreateDataIntegrationSchedule",
        "app-integrations:StartDataIntegrationExecution",
        "app-integrations:ListDataIntegrationExecutions",
        "app-integrations:GetDataIntegrationExecution",
        "app-integrations:ListDataIntegrationSchedules",
        "app-integrations:UpdateDataIntegrationSchedule",
        "app-integrations:GetDataIntegrationSchedule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:*"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "DenyWisdomForConnectEnabledTaggedResources",
      "Effect" : "Deny",
      "Action" : [
        "wisdom:DeleteAssistant",
        "wisdom:DeleteKnowledgeBase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowListOperationForWisdom",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSListRetirableGrants",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage",
        "sms-voice:DescribePhoneNumbers"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowCognitoForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:ListUserPoolClients"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorGetOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorListOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:ListVoiceConnectors"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESPermissionsForManagingReceiptRules",
      "Effect" : "Allow",
      "Action" : [
        "ses:DescribeReceiptRule",
        "ses:UpdateReceiptRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESPermissionForManagingConnectProvidedSESIdentity",
      "Effect" : "Allow",
      "Action" : [
        "ses:DeleteEmailIdentity"
      ],
      "Resource" : "arn:aws:ses:*:*:identity/*.email.connect.aws*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "SESConfigurationSetPermissionsForSendingEmail",
      "Effect" : "Allow",
      "Action" : [
        "ses:SendRawEmail"
      ],
      "Resource" : "arn:aws:ses:*:*:configuration-set/configuration-set-for-connect-DO-
NOT-DELETE",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRoleToSESForReceiptRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonConnectEmailSESAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ses.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSocialMessagingOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:SendWhatsAppMessage",
        "social-messaging:PostWhatsAppMessageMedia",
        "social-messaging:GetWhatsAppMessageMedia",
        "social-messaging:GetLinkedWhatsAppBusinessAccountPhoneNumber"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:phone-number-id/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
```

```
        }
      }
    },
    {
      "Sid" : "AllowRetrievalOfWabas",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:ListLinkedWhatsAppBusinessAccounts"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrievalOfWhatsAppTemplates",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:GetWhatsAppMessageTemplate",
        "social-messaging:ListWhatsAppMessageTemplates"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:waba/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowMobileTargetingOperationsForConnect",
      "Effect" : "Allow",
      "Action" : "mobiletargeting:SendMessages",
      "Resource" : "arn:aws:mobiletargeting:*:*:apps/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPollyActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "polly:ListLexicons",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonConnectSynchronizationServiceRolePolicy

Descrizione: consente ad Amazon Connect di sincronizzare AWS le risorse tra le regioni per tuo conto.

`AmazonConnectSynchronizationServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 27 ottobre 2023, 22:38 UTC
- Ora modificata: 21 novembre 2025, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:Create*",
        "connect:BatchCreate*",
        "connect:Update*",
        "connect:BatchUpdate*",
        "connect:Delete*",
        "connect:BatchDelete*",
        "connect:Describe*",
        "connect:BatchDescribe*",
        "connect:List*",
        "connect:Search*",
        "connect:Associate*",
        "connect:Disassociate*",
        "connect:Get*",
        "connect:BatchGet*",
        "connect:Import*",
        "connect:TagResource",
        "connect:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DisallowedConnectActions",
      "Effect" : "Deny",
      "Action" : [
        "connect:Start*",
        "connect:Stop*",
```

```
        "connect:Resume*",
        "connect:Suspend*",
        "connect:*Contact",
        "connect:SearchContacts",
        "connect:*ContactAttributes*",
        "connect:*RealtimeContact*",
        "connect:*AnalyticsData*",
        "connect:*MetricData*",
        "connect:*UserData*",
        "connect:*ContactEvaluation",
        "connect:*AttachedFile*",
        "connect:UpdateContactSchedule",
        "connect:UpdateContactRoutingData",
        "connect:ListContactReferences",
        "connect:CreateParticipant",
        "connect:CreatePersistentContactAssociation",
        "connect:CreateInstance",
        "connect:DeleteInstance",
        "connect:ListInstances",
        "connect:ReplicateInstance",
        "connect:GetFederationToken",
        "connect:ClaimPhoneNumber",
        "connect:ImportPhoneNumber",
        "connect:ReleasePhoneNumber",
        "connect:SearchAvailablePhoneNumbers",
        "connect:CreateTrafficDistributionGroup",
        "connect:DeleteTrafficDistributionGroup",
        "connect:GetTrafficDistribution",
        "connect:UpdateTrafficDistribution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonConnectVoiceIDFullAccess

Descrizione: Fornisce accesso completo a Amazon Connect Voice ID

`AmazonConnectVoiceIDFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonConnectVoiceIDFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 settembre 2021, 19:04 UTC
- Ora modificata: 26 settembre 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "voiceid:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneBedrockModelConsumptionPolicy

Descrizione: fornisce le autorizzazioni per utilizzare i modelli Amazon Bedrock, incluso il richiamo del profilo di inferenza dell'applicazione Amazon Bedrock creato per un particolare dominio Amazon. DataZone

`AmazonDataZoneBedrockModelConsumptionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneBedrockModelConsumptionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 novembre 2024, 22:15 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelConsumptionPolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InvokeDomainInferenceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "ListFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockCreateSessionWithTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "bedrock:CreateSession",
        "bedrock:TagResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:RequestTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:RequestTag/AmazonDataZoneDomain" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetSession",
        "bedrock:UpdateSession",
        "bedrock:DeleteSession",
        "bedrock:EndSession",
        "bedrock:CreateInvocation",
        "bedrock:ListInvocations",
        "bedrock:PutInvocationStep",
        "bedrock:GetInvocationStep",
        "bedrock:ListInvocationSteps",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockListSessionsPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListSessions",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneBedrockModelManagementPolicy

Descrizione: fornisce le autorizzazioni per gestire l'accesso al modello Amazon Bedrock, inclusa la creazione, l'etichettatura e l'eliminazione dei profili di inferenza delle applicazioni.

`AmazonDataZoneBedrockModelManagementPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneBedrockModelManagementPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 novembre 2024, 22:14 UTC
- Ora modificata: 12 novembre 2024, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelManagementPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingBedrockModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
```

```
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneDomainExecutionRolePolicy

Descrizione: politica predefinita per il ruolo DataZone di DomainExecutionRole servizio di Amazon. Questo ruolo viene utilizzato da Amazon DataZone per catalogare, scoprire, gestire, condividere e analizzare i dati nel DataZone dominio Amazon.

`AmazonDataZoneDomainExecutionRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneDomainExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 settembre 2023, 21:55 UTC
- Ora modificata: 26 febbraio 2026, 00:12 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
```

```
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
```

```
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:QueryGraph",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
```

```
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneEnvironmentRolePermissionsBoundary

Descrizione: Amazon DataZone crea ruoli IAM for Environments per eseguire azioni di analisi dei dati e utilizza questa policy durante la creazione di questi ruoli per definire i limiti delle loro autorizzazioni.

`AmazonDataZoneEnvironmentRolePermissionsBoundary`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneEnvironmentRolePermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 settembre 2023, 23:38 UTC
- Ora modificata: 17 novembre 2023, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateGlueConnection",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
```

```
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SameAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AnalyticsOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QueryOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
```

```
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:Describe*",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
```

```
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
```

```
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QueryOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryResultsStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsManagerOperationsWithTagKeys",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "*",
          "aws:ResourceTag/AmazonDataZoneProject" : "*"
```

```
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid" : "DataZoneS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/datazone/*"
      ]
    },
    {
      "Sid" : "DataZoneS3BucketLocation",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListDataZoneS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "datazone:*",
        "sqlworkbench:*",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
```

```
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
```

```
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:List*",
```

```
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
```

```
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneFullAccess

Descrizione: Fornisce l'accesso completo ad Amazon DataZone tramite l'accesso limitato ai servizi correlati da esso richiesti. Console di gestione AWS

`AmazonDataZoneFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 settembre 2023, 20:06 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
```

```
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
        "aoss:ListSecurityPolicies"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
```

```
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
```

```
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ConnectionStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
```

```
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "genai-studio-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
```

```
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
```

```
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneFullUserAccess

Descrizione: fornisce l'accesso completo ad Amazon DataZone, ma non consente la gestione di domini, utenti o account associati.

`AmazonDataZoneFullUserAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneFullUserAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 settembre 2023, 21:06 UTC
- Ora modificata: 19 novembre 2024, 21:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
```

```
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetIamPortalLoginUrl",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
```

```
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:PostTimeSeriesDataPoints",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
```

```
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareOperations",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneGlueManageAccessRolePolicy

Descrizione: la politica concede le autorizzazioni per consentire ad Amazon di DataZone abilitare la pubblicazione e le concessioni di accesso ai dati.

`AmazonDataZoneGlueManageAccessRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneGlueManageAccessRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 settembre 2023, 20:21 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Versione della politica

Versione della politica: v18 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueTagDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "ForAnyValue:StringLikeIfExists" : {
          "aws:TagKeys" : "DataZoneDiscoverable_*"
        }
      }
    },
    {
      "Sid" : "GlueDataQuality",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListDataQualityResults",
        "glue:GetDataQualityResult"
      ],
      "Resource" : "arn:aws:glue:*:*:dataQualityRuleset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueCrawler",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnection",
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "GlueTableDatabaseCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:CreateCatalog",
        "glue:CreateDatabase",
        "glue:DeleteCatalog",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGetTags",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "LakeformationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:UpdateDataCellsFilter",
        "glue:GetDatabase",
        "glue:GetTable",
        "organizations:DescribeOrganization",
        "ram:GetResourceShareInvitations",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LakeformationResourceFederatedSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "lakeformation:GlueARN" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShares",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/datazone:projectId" : "proj-all"
        }
      }
    },
    {
      "Sid" : "GetRoleForDataZone",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*"
      ]
```

```
    },
    {
      "Sid" : "PassRoleForDataLocationRegistration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/datazone_usr_role*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lakeformation.amazonaws.com",
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCatalogEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateCatalogS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
```

```
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZonePortalFullAccessPolicy

Descrizione: Fornisce accesso completo ad Amazon DataZone APIs

`AmazonDataZonePortalFullAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZonePortalFullAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 marzo 2023, 18:24 UTC
- Ora modificata: 26 marzo 2023, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "datazonecontrol:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZonePreviewConsoleFullAccess

Descrizione: fornisce l'accesso completo alla versione di anteprima di Amazon DataZone tramite Console di gestione AWS. Fornisce inoltre un accesso selezionato ad altri servizi correlati.

`AmazonDataZonePreviewConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZonePreviewConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 marzo 2023, 15:16 UTC
- Ora modificata: 13 luglio 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datazonecontrol:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "glue:GetConnections",
        "glue:GetDatabase",
        "redshift:DescribeClusters",
        "ec2:DescribeSubnets",
        "secretsmanager:ListSecrets",
        "iam:ListRoles",
```

```
        "sso:DescribeRegisteredRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AmazonDataZone-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneBootstrapServicePolicy-
AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneServicePolicy-
AmazonDataZoneServiceRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/AmazonDataZoneBootstrapRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:role/AmazonDataZoneDomainExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneDomainExecutionRole"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazonecontrol.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneProjectDeploymentPermissionsBoundary

Descrizione: Amazon DataZone crea ruoli IAM che utilizza per distribuire progetti di analisi dei dati. DataZone utilizza questa politica durante la creazione di questi ruoli per definire i limiti delle relative autorizzazioni.

`AmazonDataZoneProjectDeploymentPermissionsBoundary`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneProjectDeploymentPermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 marzo 2023, 02:54 UTC
- Ora modificata: 04 aprile 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneProjectRolePermissionsBoundary"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
```

```
        "kms:TagResource",
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:CreateLogGroup",
        "logs:TagLogGroup",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:*"
        },
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "kms:ScheduleKeyDeletion",
        "kms:DescribeKey",
        "kms:EnableKeyRotation",
        "kms:DisableKeyRotation",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:projectId"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "s3:DeleteBucket"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:s3:::datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:RevokePermissions",
```

```
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:PutBucketLogging",
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*"
      ],
      "Resource" : "arn:aws:s3:::*datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:Get*",
        "athena:List*",
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:Describe*",
        "ec2:Get*",
        "ec2:List*",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "logs:DeleteLogGroup",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:PutKeyPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.logs",
            "com.amazonaws.*.s3",
            "com.amazonaws.*.glue",
            "com.amazonaws.*.athena"
          ]
        }
      }
    },
    {
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:TagResource",
        "cloudformation:GetTemplateSummary"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*",
        "s3:DeleteBucket"
      ],
      "NotResource" : [
```

```
        "arn:aws:s3:::*datazone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:DeleteBucket",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicy",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
```

```
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplateSummary",
        "athena:*",
        "kms:*",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "lambda:*",
        "ec2:*",
        "logs:*",
        "servicecatalog:CreateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:GetApplication",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:PassRole",
        "iam:TagRole",
        "s3:GetBucket*",
        "s3:GetObject*",
        "s3:Abort*",
        "s3:GetEncryptionConfiguration",
        "s3:PutObject*"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneProjectRolePermissionsBoundary

Descrizione: Amazon DataZone crea ruoli IAM per i progetti per eseguire azioni di analisi dei dati e utilizza questa policy durante la creazione di questi ruoli per definire i limiti delle loro autorizzazioni.

`AmazonDataZoneProjectRolePermissionsBoundary`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneProjectRolePermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 marzo 2023, 02:51 UTC
- Ora modificata: 21 marzo 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "logs:*",
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGet*",
        "athena:List*",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:Get*",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
```

```
        "ram:CreateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:AcceptResourceShareInvitation",
        "ram:Get*",
        "ram:List*",
        "redshift:DescribeClusters",
        "redshift:JoinGroup",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift-data:*",
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares",
        "redshift:AssociateDataShareConsumer",
        "tag:GetResources",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "glue:CreateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateDataQualityRuleset",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateWorkflow",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/datazone:projectId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:BatchGet*",
        "glue:SearchTables",
        "glue:List*",
        "glue:Get*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:DeleteResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
```

```
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "logs:*",
        "athena:*",
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
```

```
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:*",
        "redshift:*",
        "redshift-data:*",
        "tag:GetResources",
        "iam:List*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:PassRole",
```

```
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneRedshiftGlueProvisioningPolicy

Descrizione: Amazon DataZone è un servizio di gestione dei dati che ti consente di catalogare, scoprire, governare, condividere e analizzare i tuoi dati. Con Amazon DataZone, puoi condividere e accedere ai tuoi dati tra account e regioni supportate. Amazon DataZone semplifica la tua esperienza con tutti AWS i servizi, inclusi, a titolo esemplificativo, Amazon Redshift, Amazon Athena, AWS Glue e Lake Formation. AWS

`AmazonDataZoneRedshiftGlueProvisioningPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneRedshiftGlueProvisioningPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 settembre 2023, 20:19 UTC
- Ora modificata: 23 ottobre 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackCreationForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackManagementForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "athena:GetWorkGroup",
        "logs:DescribeLogGroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift:DescribeClusters",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource",
```

```
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:TagLogGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupCreation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupManagement",
      "Action" : [
```

```
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentIAMPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:GetPolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentS3ValidationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSDecryptPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "RedshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ListSchemas",
        "redshift-data:ExecuteStatement"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "DescribeStatementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSecretValuePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneRedshiftManageAccessRolePolicy

Descrizione: questa policy concede ad Amazon DataZone le autorizzazioni per pubblicare i dati di Amazon Redshift nel catalogo. Fornisce inoltre ad Amazon DataZone le autorizzazioni per concedere o revocare l'accesso agli asset pubblicati di Amazon Redshift o Amazon Redshift Serverless nel catalogo.

`AmazonDataZoneRedshiftManageAccessRolePolicy`AWS è una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneRedshiftManageAccessRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 settembre 2023, 20:15 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "redshiftDataScopeDownPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift-data:BatchExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "listSecretsPermission",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "getWorkgroupPermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetWorkgroup",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteWorkgroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteWorkgroup"
      ],
      "Resource" : [
```

```
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "getNamespacePermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetNamespace",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:DeleteNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
```

```
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "redshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "dataSharesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "associateDataShareConsumerPermission",
      "Effect" : "Allow",
      "Action" : "redshift:AssociateDataShareConsumer",
      "Resource" : "arn:aws:redshift:*:*:datashare:*/datazone*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

Descrizione: la AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary policy è l'elenco delle autorizzazioni consentite su un ruolo di esecuzione creato in un SageMaker ambiente fornito da Amazon. DataZone

`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 aprile 2024, 23:01 UTC
- Ora modificata: 17 luglio 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`

Versione della politica

Versione della politica: v13 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "AllowSageMakerProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile",
        "sagemaker:UpdateUserProfile",
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:*/*"
    },
    {
      "Sid" : "AllowLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsForDomainResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
```

```
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateApp",
            "CreateSpace",
            "CreateUserProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListSpaces",
        "sagemaker:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
```

```
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*",
        "datazone:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:Describe*",
```

```
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "groundtruthlabeling:*",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
```

```
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowRAMInvitation",
      "Effect" : "Allow",
      "Action" : "ram:AcceptResourceShareInvitation",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "dzd*"
        }
      }
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker*",
        "arn:aws:ecr:*:*:repository/datazone*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
```

```
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ]
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ]
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
```

```
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
```

```
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "states.amazonaws.com",
            "lakeformation.amazonaws.com",
            "events.amazonaws.com",
            "sagemaker.amazonaws.com",
            "forecast.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CrossAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
```

```
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:domain/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:ListJobs",
```

```
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:GetTable",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:ListSchemas",
        "glue:BatchGetJobs",
        "glue:GetConnection",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "AllowGlueActionsWithEnvironmentTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:ListSchemas",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "AllowGlueDefaultAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:RunStatement"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:connection/dz-sm-*",
        "arn:aws:glue:*:*:session/*"
      ]
    },
    {
      "Sid" : "AllowRedshiftClusterActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowCreateClusterUser",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterUser"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*"
      ]
    },
    {
      "Sid" : "AllowCreateSecretActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
```

```
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventBridgeRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEMR",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSOAction",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DenyNotAction",
      "Effect" : "Deny",
      "NotAction" : [
        "sagemaker:*",
        "sagemaker-geospatial:*",
        "sqlworkbench:*",
        "datazone:*",
        "forecast:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
```

```
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:StartImageScan",
        "ecr:TagResource",
        "ecr:UntagResource",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters",
        "events:PutRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:TagResource",
        "events:ListTagsForResource",
        "fsx:DescribeFileSystems",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
```

```
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGet*",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:Get*",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:List*",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreateDatabase",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "groundtruthlabeling:*",
```

```
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant",
        "lakeformation:GetDataAccess",
        "lambda:ListFunctions",
        "lambda:InvokeFunction",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "ram:AcceptResourceShareInvitation",
        "rds:DescribeDBInstances",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:GetBucketAcl",
```

```
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors",
        "s3:DeleteObjectVersion",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:TagResource",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine",
        "tag:GetResources",
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DenyUpdateNotebookInstanceLifecycleConfig",
      "Effect" : "Deny",
      "Action" : [
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneSageMakerManageAccessRolePolicy

Descrizione: la AmazonDataZoneSageMakerManageAccessRolePolicy policy concede ad Amazon DataZone le autorizzazioni necessarie per concedere agli utenti l'accesso a varie risorse dell' SageMaker ambiente.

`AmazonDataZoneSageMakerManageAccessRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneSageMakerManageAccessRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 aprile 2024, 23:34 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:ListTags",
        "sagemaker:DescribeDomain",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
```

```
          "aws:TagKeys" : [
            "sagemaker:shared-with:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelPackageGroupPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:DeleteModelPackageGroupPolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerRAMResourcePolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutResourcePolicy",
        "sagemaker:GetResourcePolicy",
        "sagemaker:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:feature-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMTagResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
```

```
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMDeleteResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMCreateResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "sagemaker:*"
          ]
        },
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerS3BucketPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucketPolicy",
```

```
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetRepositoryPolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:DeleteRepositoryPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonSageMakerKMSReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSGrantPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDataZoneSageMakerProvisioningRolePolicy

Descrizione: la AmazonDataZoneSageMakerProvisioningRolePolicy politica concede ad Amazon DataZone le autorizzazioni necessarie per interagire con Amazon. SageMaker

`AmazonDataZoneSageMakerProvisioningRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonDataZoneSageMakerProvisioningRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 aprile 2024, 23:32 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false",
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
```

```
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ],
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "sagemaker:ListDomains"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSKeyValidation",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection",
        "glue:GetConnection"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDetectiveFullAccess

Descrizione: Fornisce accesso completo al servizio Amazon Detective e accesso mirato alle dipendenze dell'interfaccia utente della console

`AmazonDetectiveFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDetectiveFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 aprile 2020, 17:57 UTC

- Ora modificata: 17 maggio 2023, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:*",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings"
      ],
      "Resource" : "arn:aws:guardduty:*:*:detector/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDetectiveInvestigatorAccess

Descrizione: fornisce agli investigatori l'accesso al servizio Amazon Detective e l'accesso mirato alle dipendenze dell'interfaccia utente della console. Questa politica concede il permesso di immergersi in Detective per scopi investigativi e un accesso scritto limitato a Guardduty.

`AmazonDetectiveInvestigatorAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDetectiveInvestigatorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 gennaio 2023, 15:24 UTC
- Ora modificata: 27 novembre 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DetectivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDetectiveMemberAccess

Descrizione: fornisce ai membri l'accesso al servizio Amazon Detective e l'accesso mirato alle dipendenze dell'interfaccia utente della console.

`AmazonDetectiveMemberAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDetectiveMemberAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 gennaio 2023, 15:16 UTC
- Ora modificata: 17 gennaio 2023, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDetectiveOrganizationsAccess

Descrizione: Fornisce alle Organizzazioni l'accesso alla gestione dell'amministratore delegato per Amazon Detective e l'accesso mirato alle dipendenze dell'interfaccia utente della console. Ciò concede anche l'autorizzazione a creare un ruolo collegato al servizio per Detective.

`AmazonDetectiveOrganizationsAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonDetectiveOrganizationsAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 marzo 2023, 15:20 UTC
- Ora modificata: 2 marzo 2023, 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDetectiveServiceLinkedRolePolicy

Descrizione: consente ad Amazon Detective di effettuare chiamate di assistenza per tuo conto

`AmazonDetectiveServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 novembre 2021, 19:47 UTC
- Ora modificata: 18 novembre 2021, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDevOpsGuruConsoleFullAccess

Descrizione: la policy garantisce l'accesso completo alla console DevOps Guru.

`AmazonDevOpsGuruConsoleFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonDevOpsGuruConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 dicembre 2021, 18:43 UTC
- Ora modificata: 25 agosto 2022, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PerformanceInsightsMetricsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics",
        "pi:DescribeDimensionKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDevOpsGuruFullAccess

Descrizione: Fornisce l'accesso completo ad Amazon DevOps Guru.

`AmazonDevOpsGuruFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDevOpsGuruFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 16:38 UTC
- Ora modificata: 25 agosto 2022, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDevOpsGuruOrganizationsAccess

Descrizione: Fornisci l'accesso per abilitare e gestire Amazon DevOps Guru all'interno di un'organizzazione.

`AmazonDevOpsGuruOrganizationsAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDevOpsGuruOrganizationsAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2021, 23:50 UTC
- Ora modificata: 15 novembre 2021, 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:SearchOrganizationInsights"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "arn:aws:organizations::*:"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "devops-guru.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDevOpsGuruReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alla console Amazon DevOps Guru.

`AmazonDevOpsGuruReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDevOpsGuruReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 16:34 UTC

- Ora modificata: 25 agosto 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDevOpsGuruServiceRolePolicy

Descrizione: un ruolo collegato al servizio richiesto ad Amazon DevOpsGuru per accedere alle tue risorse.

`AmazonDevOpsGuruServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 01 dicembre 2020, 10:24 UTC
- Ora modificata: 10 gennaio 2023, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudtrail:LookupEvents",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListDashboards",
        "cloudwatch:GetDashboard",
        "cloudformation:GetTemplate",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",
        "config:DescribeConfigurationRecorderStatus",
        "config:GetResourceConfigHistory",
        "events:ListRuleNamesByTarget",
        "xray:GetServiceGraph",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "pi:GetResourceMetrics",
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
        "lambda:GetAccountSettings",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
```

```
        "lambda:GetPolicy",
        "ec2:DescribeSubnets",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "sqs:GetQueueAttributes",
        "kinesis:DescribeStream",
        "kinesis:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeStream",
        "dynamodb:ListStreams",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeAccountAttributes",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketWebsite",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListStorageLensConfigurations",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutTargetsOnASpecificRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
    },
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsToOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCreateManagedRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
    {
      "Sid" : "AllowAccessManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
```

```
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
    {
      "Sid" : "AllowOtherOperationsOnManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowTagBasedFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAPIGatewayGetIntegrations",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/??????????",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
      ]
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDMSCloudWatchLogsRole

Descrizione: fornisce l'accesso per caricare i log di replica DMS sui log di cloudwatch nell'account del cliente.

`AmazonDMSCloudWatchLogsRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonDMSCloudWatchLogsRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 gennaio 2016, 23:44 UTC
- Ora modificata: 23 maggio 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AllowDescribeOnAllLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeOfAllLogStreamsOnDmsTasksLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
```

```
    },
    {
      "Sid" : "AllowUploadOfLogEventsToDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDMSRedshiftS3Role

Descrizione: fornisce l'accesso per gestire le impostazioni S3 per gli endpoint Redshift per DMS.

`AmazonDMSRedshiftS3Role`è una policy gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonDMSRedshiftS3Role` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2016, 17:05 UTC
- Ora modificata: 08 luglio 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:DeleteBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutBucketVersioning",
        "s3:GetBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:DeleteBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::dms-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDMSVPCManagementRole

Descrizione: Fornisce l'accesso alla gestione delle impostazioni VPC per le configurazioni AWS gestite dei clienti

`AmazonDMSVPCManagementRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDMSVPCManagementRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 18 novembre 2015, 16:33 UTC
- Ora modificata: 25 luglio 2024, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDocDB-ElasticServiceRolePolicy

Descrizione: consente ad Amazon DocumentDB-Elastic di gestire AWS le risorse per tuo conto.

`AmazonDocDB-ElasticServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 30 novembre 2022, 14:17 UTC
- Ora modificata: 30 novembre 2022, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Elastic"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDocDBConsoleFullAccess

Descrizione: fornisce l'accesso completo per gestire Amazon DocumentDB con compatibilità con MongoDB utilizzando. Console di gestione AWS Tieni presente che questa politica garantisce anche l'accesso completo alla pubblicazione su tutti gli argomenti SNS all'interno dell'account, le autorizzazioni per creare e modificare istanze Amazon EC2 e configurazioni VPC, le autorizzazioni per visualizzare ed elencare le chiavi su Amazon KMS e l'accesso completo ad Amazon RDS e Amazon Neptune.

`AmazonDocDBConsoleFullAccess`è una AWS politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDocDBConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 gennaio 2019, 20:37 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbSids",
      "Effect" : "Allow",
      "Action" : [
```

```
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
```

```
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DependencySids",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DocdbSLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DocdbElasticSLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDocDBElasticFullAccess

Descrizione: fornisce l'accesso completo ad Amazon DocumentDB Elastic Clusters e ad altre autorizzazioni richieste per le sue dipendenze, tra cui EC2, KMS e IAM. SecretsManager CloudWatch

`AmazonDocDBElasticFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonDocDBElasticFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 giugno 2023, 13:51 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbElasticSid",
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Sid",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ],
          "aws:ResourceTag/DocDBElasticFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "KMSGrantSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/DocDBElasticFullAccess" : "*",
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
```

```
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "SecretManagerSid",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudwatchSid",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDocDBElasticReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon DocDB-Elastic e ai parametri. CloudWatch

`AmazonDocDBElasticReadOnlyAccess`AWS è una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDocDBElasticReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 giugno 2023, 14:37 UTC
- Ora modificata: 21 giugno 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:ListClusters",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDocDBFullAccess

Descrizione: fornisce l'accesso completo ad Amazon DocumentDB con compatibilità con MongoDB. Tieni presente che questa politica garantisce anche l'accesso completo alla pubblicazione su tutti gli argomenti SNS all'interno dell'account e l'accesso completo ad Amazon RDS e Amazon Neptune.

`AmazonDocDBFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonDocDBFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 gennaio 2019, 20:21 UTC
- Ora modificata: 09 gennaio 2019, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
```

```
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
```

```
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDocDBReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon DocumentDB con compatibilità con MongoDB. Tieni presente che questa politica consente anche l'accesso alle risorse di Amazon RDS e Amazon Neptune.

`AmazonDocDBReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonDocDBReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 gennaio 2019, 20:30 UTC
- Ora modificata: 09 gennaio 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDRSVPCManagement

Descrizione: Fornisce l'accesso per gestire le impostazioni VPC per le configurazioni gestite dai clienti di Amazon

`AmazonDRSVPCManagement`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDRSVPCManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 settembre 2015, 00:09 UTC
- Ora modificata: 02 settembre 2015, 00:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDynamoDBFullAccess

Descrizione: fornisce l'accesso completo ad Amazon DynamoDB tramite. Console di gestione AWS

`AmazonDynamoDBFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDynamoDBFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 29 gennaio 2021, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "dynamodb:*",
        "dax:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:GetMetricData",
        "datapipeline:ActivatePipeline",
```

```
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes",
        "lambda:CreateFunction",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetFunctionConfiguration",
        "lambda:DeleteFunction",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "resource-groups:DeleteGroup",
        "resource-groups:CreateGroup",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn",
            "dax.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDynamoDBFullAccess_v2

Descrizione: Fornisce accesso completo ad Amazon DynamoDB

`AmazonDynamoDBFullAccess_v2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDynamoDBFullAccess_v2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 maggio 2025, 14:52 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess_v2`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "DDBAndDAXFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:*",
        "dax:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaIntegration",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DaxSNSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchMonitoring",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListKinesisResources",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ListEC2ResourcesForDaxClusterCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchInsightsRules",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Sid" : "ServiceRoleCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDynamoDBFullAccesswithDataPipeline

Descrizione: questa politica si trova su un percorso obsoleto. Consulta la documentazione come guida: https://docs.aws.amazon.com/amazondynamodb/ latest/developerguide/ DynamoDBPipeline.html. Provides full access to Amazon DynamoDB including Export/Import utilizzo di AWS Data Pipeline tramite. Console di gestione AWS

`AmazonDynamoDBFullAccesswithDataPipeline`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDynamoDBFullAccesswithDataPipeline` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 12 novembre 2015, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:*",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsole"
    },
    {
      "Action" : [
        "lambda:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleTriggers"
    },
    {
      "Action" : [
```

```
        "datapipeline:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleImportExport"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRolePolicy",
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Sid" : "IAMEDPRoles"
    },
    {
      "Action" : [
        "ec2:CreateTags",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "EMR"
    },
    {
      "Action" : [
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:Put*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
```

```
      "Sid" : "S3"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonDynamoDBReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon DynamoDB tramite. Console di gestione AWS

`AmazonDynamoDBReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonDynamoDBReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 18 novembre 2024, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetAbacStatus",
        "dynamodb:GetItem",
        "dynamodb:GetResourcePolicy",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dax:Describe*",
        "dax:List*",
        "dax:GetItem",
        "dax:BatchGetItem",
        "dax:Query",
        "dax:Scan",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
```

```
        "kms:ListAliases",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:GetFunctionConfiguration",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CCIAccess",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEBSCSIDriverEKSClusterScopedPolicy

Descrizione: politica IAM che consente all'account del servizio driver CSI di effettuare chiamate a servizi correlati come EC2 per tuo conto. Questa policy limita il driver CSI di Amazon EBS alla gestione solo di volumi e snapshot EBS che appartengono a un cluster EKS specifico. Richiede il tag di risorsa ebs.csi.aws. com/cluster-name deve corrispondere al tag eks-cluster-name sul principale

IAM, impedendo l'accesso tra cluster quando più cluster condividono lo stesso. Account AWS Le operazioni di collegamento e scollegamento sulle istanze sono limitate alle istanze etichettate con il tag eks:cluster-name (impostato automaticamente da EKS sui gruppi di nodi gestiti) o ebs.csi.aws.com/cluster-name tag (per le istanze con tag manualmente).

`AmazonEBSCSIDriverEKSClusterScopedPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEBSCSIDriverEKSClusterScopedPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 aprile 2026, 17:27 UTC
- Ora modificata: 28 maggio 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEBSCSIDriverEKSClusterScopedPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSnapshots",
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateAndCopyVolumesWithClusterTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CopyClusterVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithClusterTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsFromClusterVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "ManageClusterVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CreateVolumesFromAndEnableFSROnClusterSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToClusterInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:cluster-name" : "${aws:PrincipalTag/eks-cluster-name}"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToEKSStandardTaggedInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks-cluster-
name}"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToManuallyTaggedInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "DeleteAndLockClusterSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "TagResourcesOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
      "Sid" : "ModifyTagsOnClusterVolumes",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "ebs.csi.aws.com/cluster",
            "ebs.csi.aws.com/cluster-name",
            "kubernetes.io/created-for/pvc/name"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEBSCSIDriverPolicy

Descrizione: politica IAM che consente all'account del servizio driver CSI di effettuare chiamate a servizi correlati come EC2 per tuo conto.

`AmazonEBSCSIDriverPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEBSCSIDriverPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 4 aprile 2022, 17:24 UTC
- Ora modificata: 13 maggio 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/vol-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeName" : "*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:RequestTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEBSCSIDriverPolicyV2

Descrizione: politica IAM che consente all'account del servizio driver CSI EBS di effettuare chiamate a servizi correlati come EC2 per tuo conto. Limita il driver CSI di Amazon EBS alla gestione solo di volumi e snapshot EBS etichettati con la chiave ebs.csi.aws. com/cluster set to true. Volumes provisioned by the in-tree Kubernetes volume plugin (CSI-migrated volumes) are also supported through the kubernetes.io/created-for/pvc/nametag di risorsa.

`AmazonEBSCSIDriverPolicyV2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEBSCSIDriverPolicyV2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 aprile 2026, 17:27 UTC
- Ora modificata: 16 aprile 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEBSCSIDriverPolicyV2`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateAndCopyVolumesWithManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "CopyManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "CopyCSIMigratedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsFromManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "ManageManagedVolumes",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "ManageCSIMigratedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Sid" : "CreateVolumesFromAndEnableFSROnManagedSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "AttachDetachVolumesToAnyInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteAndLockManagedSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "TagResourcesOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "ModifyTagsOnManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "ebs.csi.aws.com/cluster",
            "ebs.csi.aws.com/cluster-name",
            "kubernetes.io/created-for/pvc/name"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2ContainerRegistryFullAccess

Descrizione: Fornisce accesso amministrativo alle risorse Amazon ECR

`AmazonEC2ContainerRegistryFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2ContainerRegistryFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 dicembre 2015, 17:06 UTC
- Ora modificata: 05 dicembre 2020, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.ecr.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2ContainerRegistryPowerUser

Descrizione: fornisce l'accesso completo ai repository di Amazon EC2 Container Registry, ma non consente l'eliminazione degli archivi o la modifica delle policy.

`AmazonEC2ContainerRegistryPowerUser`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2ContainerRegistryPowerUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 dicembre 2015, 17:05 UTC
- Ora modificata: 10 dicembre 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2ContainerRegistryPullOnly

Descrizione: fornisce l'accesso per estrarre immagini dai repository di Amazon EC2 Container Registry.

`AmazonEC2ContainerRegistryPullOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2ContainerRegistryPullOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 ottobre 2024, 16:58 UTC
- Ora modificata: 04 ottobre 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchImportUpstreamImage"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2ContainerRegistryReadOnly

Descrizione: fornisce accesso in sola lettura ai repository di Amazon EC2 Container Registry.

`AmazonEC2ContainerRegistryReadOnly`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2ContainerRegistryReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 dicembre 2015, 17:04 UTC
- Ora modificata: 10 dicembre 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2ContainerServiceAutoscaleRole

Descrizione: policy per abilitare Task Autoscaling per Amazon EC2 Container Service

`AmazonEC2ContainerServiceAutoscaleRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2ContainerServiceAutoscaleRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 maggio 2016, 23:25 UTC
- Ora modificata: 5 febbraio 2018, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2ContainerServiceEventsRole

Descrizione: Politica per abilitare CloudWatch Events for EC2 Container Service

`AmazonEC2ContainerServiceEventsRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2ContainerServiceEventsRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 30 maggio 2017, 16:51 UTC
- Ora modificata: 6 marzo 2023, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RunTask"
          ]
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2ContainerServiceforEC2Role

Descrizione: policy predefinita per il ruolo Amazon EC2 per Amazon EC2 Container Service.

`AmazonEC2ContainerServiceforEC2Role`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2ContainerServiceforEC2Role` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 marzo 2015, 18:45 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ecs:CreateCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:DiscoverPollEndpoint",
        "ecs:Poll",
        "ecs:RegisterContainerInstance",
        "ecs:StartTelemetrySession",
        "ecs:UpdateContainerInstancesState",
        "ecs:Submit*",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterContainerInstance"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTagsForResource"
```

```
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*",
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2ContainerServiceRole

Descrizione: policy predefinita per il ruolo del servizio Amazon ECS.

`AmazonEC2ContainerServiceRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2ContainerServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 9 aprile 2015, 16:14 UTC
- Ora modificata: 11 agosto 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2FullAccess

Descrizione: fornisce l'accesso completo ad Amazon EC2 tramite. Console di gestione AWS

`AmazonEC2FullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 27 novembre 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "ec2:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:*",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "ec2scheduled.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2ImageReferencesAccessPolicy

Descrizione: fornisce l'accesso in sola lettura per scansionare tutti i tipi di risorse supportati alla ricerca di dati pertinenti durante l'utilizzo. DescribeImageReferences

`AmazonEC2ImageReferencesAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2ImageReferencesAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 agosto 2025, 19:19 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ImageReferencesAccessPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:DescribeImageReferences",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ssm:DescribeParameters",
        "ssm:GetParameters",
        "imagebuilder:ListImageRecipes",
```

```
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:GetContainerRecipe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ec2-images.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2ReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon EC2 tramite. Console di gestione AWS

`AmazonEC2ReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2ReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2RoleforAWSCodeDeploy

Descrizione: fornisce l'accesso EC2 al bucket S3 per scaricare la revisione. Questo ruolo è necessario all' CodeDeploy agente sulle istanze EC2.

`AmazonEC2RoleforAWSCodeDeploy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2RoleforAWSCodeDeploy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 maggio 2015, 18:10 UTC
- Ora modificata: 20 marzo 2017, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2RoleforAWSCodeDeployLimited

Descrizione: fornisce a EC2 un accesso limitato al bucket S3 per scaricare la revisione. Questo ruolo è necessario all' CodeDeploy agente sulle istanze EC2.

`AmazonEC2RoleforAWSCodeDeployLimited`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2RoleforAWSCodeDeployLimited` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 agosto 2020, 17:55 UTC
- Ora modificata: 20 gennaio 2022, 21:37 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2RoleforDataPipelineRole

Descrizione: policy predefinita per il ruolo del servizio Amazon EC2 Role for Data Pipeline.

`AmazonEC2RoleforDataPipelineRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2RoleforDataPipelineRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 22 febbraio 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "datapipeline:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListInstance*",
        "elasticmapreduce:ModifyInstanceGroups",
        "rds:Describe*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2RoleforSSM

Descrizione: questa politica sarà presto obsoleta. Utilizza la SSMManaged InstanceCore policy di Amazon per abilitare le funzionalità principali del servizio AWS Systems Manager sulle istanze EC2. Per ulteriori informazioni, consulta -instance-profile.html https://docs.aws.amazon.com/systems-manager/ latest/userguide/setup

`AmazonEC2RoleforSSM`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2RoleforSSM` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 29 maggio 2015, 17:48 UTC
- Ora modificata: 24 gennaio 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
```

```
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetEncryptionConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2RolePolicyForLaunchWizard

Descrizione: policy gestita per il ruolo LaunchWizard di servizio Amazon per EC2

`AmazonEC2RolePolicyForLaunchWizard`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2RolePolicyForLaunchWizard` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2019, 08:05 UTC
- Ora modificata: 25 settembre 2024, 22:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceRoute"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeRouteTables",
        "ec2:ModifyInstanceAttribute",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricData",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LaunchWizardResourceGroupID",
            "LaunchWizardApplicationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketLocation",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*",
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:Create*",
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "cloudformation:DescribeStackResources",
        "cloudformation:SignalResource",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "LaunchWizardResourceGroupID"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:PutItem",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "dynamodb:Scan",
        "s3:ListBucket",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteTable",
        "dynamodb:CreateTable",
        "s3:GetObject",
        "dynamodb:DescribeTable",
        "s3:GetBucketLocation",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:dynamodb:*:*:table/LaunchWizard*",
        "arn:aws:sqs:*:*:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint",
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackintForAWSBackup"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:ListTagsForResource",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2SpotFleetAutoscaleRole

Descrizione: Policy per abilitare la scalabilità automatica per la flotta Spot di Amazon EC2

`AmazonEC2SpotFleetAutoscaleRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2SpotFleetAutoscaleRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 agosto 2016, 18:27 UTC
- Ora modificata: 18 febbraio 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEC2SpotFleetTaggingRole

Descrizione: consente a EC2 Spot Fleet di richiedere, terminare e contrassegnare istanze Spot per tuo conto.

`AmazonEC2SpotFleetTaggingRole`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonEC2SpotFleetTaggingRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 29 giugno 2017, 18:19 UTC
- Ora modificata: 23 aprile 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      },
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECS_FullAccess

Descrizione: fornisce l'accesso amministrativo alle risorse di Amazon ECS e abilita le funzionalità ECS tramite l'accesso ad altre risorse di AWS servizio VPCs, inclusi gruppi e stack di Auto Scaling. CloudFormation

`AmazonECS_FullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonECS_FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 novembre 2017, 21:36 UTC
- Ora modificata: 13 agosto 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Versione della politica

Versione della politica: v21 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSIntegrationsManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:ListMeshes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
```

```
        "autoscaling:Describe*",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ContinueDeployment",
        "codedeploy:CreateApplication",
        "codedeploy:CreateDeployment",
        "codedeploy:CreateDeploymentGroup",
        "codedeploy:GetApplication",
        "codedeploy:GetApplicationRevision",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:GetDeploymentTarget",
        "codedeploy:ListApplicationRevisions",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "codedeploy:RegisterApplicationRevision",
        "codedeploy:StopDeployment",
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateInternetGateway",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:DeleteLaunchTemplate",
```

```
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RequestSpotFleet",
        "ec2:RunInstances",
        "ecs:*",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "fsx:DescribeFileSystems",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "lambda:ListFunctions",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:FilterLogEvents",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
```

```
        "servicediscovery:CreatePrivateDnsNamespace",
        "servicediscovery:CreateService",
        "servicediscovery:DeleteService",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetOperation",
        "servicediscovery:GetService",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:UpdateService",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
    },
    {
      "Sid" : "ManagedCloudformationResourcesCleanupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteInternetGateway",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
        }
      }
    },
    {
```

```
      "Sid" : "TasksPassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InfrastructurePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInfrastructureRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstancePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AutoScalingPassRolePolicy",
      "Action" : "iam:PassRole",
```

```
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsAutoscaleRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ServiceLinkedRoleCreationPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "ecs.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.application-autoscaling.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ELBTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateTargetGroup",
            "CreateRule",
            "CreateListener",
            "CreateLoadBalancer"
```

```
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECSComputeServiceRolePolicy

Descrizione: Policy per consentire ad Amazon ECS Compute di gestire le istanze EC2 e le risorse correlate come parte delle istanze gestite ECS

`AmazonECSComputeServiceRolePolicy`è una AWS politica gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 24 marzo 2025, 17:37 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSComputeServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissionsForInstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeFleets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteManagedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TerminateManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECSInfrastructureRoleforExpressGatewayServices

Descrizione: queste autorizzazioni consentono ad Amazon ECS di fornire e gestire automaticamente i componenti dell'infrastruttura necessari per Express Gateway Services, tra cui bilanciamento del carico, gruppi di sicurezza, certificati SSL e configurazioni di scalabilità automatica.

`AmazonECSInfrastructureRoleforExpressGatewayServices`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonECSInfrastructureRoleforExpressGatewayServices` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 novembre 2025, 20:34 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRoleforExpressGatewayServices`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ServiceLinkedRoleCreateOperations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ecs.application-autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ELBOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener",
```

```
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateELBResources",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateListener",
            "CreateRule",
            "CreateTargetGroup"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "BlanketAllowCreateSecurityGroupsInVPCs",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateSecurityGroupResourcesWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifySecurityGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateEC2Resources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress",
            "AuthorizeSecurityGroupEgress"
          ]
        }
      }
    },
    {
      "Sid" : "CertificateOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate",
        "acm:AddTagsToCertificate",
        "acm:DeleteCertificate",
        "acm:DescribeCertificate"
      ],
      "Resource" : [
        "arn:aws:acm:*:*:certificate/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingCreateOperations",
      "Effect" : "Allow",
      "Action" : [
```

```
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:TagResource",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingPolicyOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "ecs"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ]
    },
    {
      "Sid" : "CloudWatchAlarmCreateOperations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchAlarmOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCReadOperations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECSInfrastructureRolePolicyForLoadBalancers

Descrizione: fornisce l'accesso ad altre risorse di AWS servizio necessarie per gestire i sistemi di bilanciamento del carico associati ai carichi di lavoro ECS per tuo conto.

`AmazonECSInfrastructureRolePolicyForLoadBalancers`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonECSInfrastructureRolePolicyForLoadBalancers` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 luglio 2025, 16:37 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForLoadBalancers`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
```

```
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
    },
    {
      "Sid" : "ALBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*"
      ]
    },
    {
      "Sid" : "NLBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/net/*/*/*"
      ]
    },
    {
      "Sid" : "ALBModifyRules",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyRule",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECSInfrastructureRolePolicyForManagedInstances

Descrizione: fornisce l'accesso ECS per creare e gestire le risorse gestite da EC2

`AmazonECSInfrastructureRolePolicyForManagedInstances`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonECSInfrastructureRolePolicyForManagedInstances` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 settembre 2025, 18:04 UTC
- Ora modificata: 26 febbraio 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForManagedInstances`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateLaunchTemplateForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateLaunchTemplateVersionsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ProvisionEC2InstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*",
```

```
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateFleetForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "RunInstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForECSManagedLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "TagOnCreateEC2ResourcesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "CreateLaunchTemplate",
            "RunInstances"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "PassInstanceRoleForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.*"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEC2Spot",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ]
    },
    {
      "Sid" : "DescribeEC2ResourcesManagedByECS",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeCapacityReservations"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ListResourceGroupResources",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

Descrizione: Fornisce l'accesso amministrativo a Private Certificate Authority, AWS Secrets Manager e ad altri elementi Servizi AWS necessari per gestire le funzionalità TLS di ECS Service Connect per tuo conto.

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 gennaio 2024, 20:08 UTC

- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
```

```
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "ManagePrivateCertificateAuthority",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true",
          "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECSInfrastructureRolePolicyForVolumes

Descrizione: fornisce l'accesso ad altre risorse AWS di servizio necessarie per gestire i volumi associati ai carichi di lavoro ECS per tuo conto.

`AmazonECSInfrastructureRolePolicyForVolumes`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonECSInfrastructureRolePolicyForVolumes` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 gennaio 2024, 22:56 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
```

```
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEBSManagedVolumeFromSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumesForLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstancesForAttachingVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ManageEBSVolumeLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECSInfrastructureRolePolicyForVpcLattice

Descrizione: Fornisce l'accesso ad altre risorse AWS di servizio necessarie per gestire la funzionalità VPC Lattice nei carichi di lavoro ECS per tuo conto.

`AmazonECSInfrastructureRolePolicyForVpcLattice`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonECSInfrastructureRolePolicyForVpcLattice` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2024, 20:02 UTC
- Ora modificata: 15 novembre 2024, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForVpcLattice`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManagedVpcLatticeTargetRegistration",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:RegisterTargets",
        "vpc-lattice:DeregisterTargets"
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "DescribeVpcLatticeTargetGroup",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:GetTargetGroup",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "ListVpcLatticeTargets",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:ListTargets",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECSInstanceRolePolicyForManagedInstances

Descrizione: policy predefinita per il ruolo dell'istanza Amazon ECS per le istanze gestite di Amazon ECS.

`AmazonECSInstanceRolePolicyForManagedInstances`è una policy gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonECSInstanceRolePolicyForManagedInstances` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 settembre 2025, 23:49 UTC
- Ora modificata: 02 luglio 2026, 02:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInstanceRolePolicyForManagedInstances`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAgentDiscoverPollEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DiscoverPollEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSAgentRegisterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterContainerInstance"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    },
    {
      "Sid" : "ECSAgentPollPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*",
        "arn:aws:ecs:*:*:task-set/*"
      ]
    },
    {
      "Sid" : "ECSAgentTelemetryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StartTelemetrySession",
        "ecs:PutSystemLogEvents"
      ],
```

```
      "Resource" : "arn:aws:ecs:*:*:container-instance/*"
    },
    {
      "Sid" : "ECSAgentStateChangePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:SubmitAttachmentStateChanges",
        "ecs:SubmitTaskStateChange"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECSServiceRolePolicy

Descrizione: policy per consentire ad Amazon ECS di gestire il cluster.

`AmazonECSServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 14 ottobre 2017, 01:18 UTC
- Ora modificata: 22 aprile 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Versione della politica

Versione della politica: v24 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:AssociateTrunkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateTrunkInterface",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:Get*",
        "route53:List*",
        "route53:UpdateHealthCheck",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:UpdateInstanceCustomHealthStatus"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:PutLifecycleHook",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling:TerminateInstanceInAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "autoscaling:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "AutoScalingPlanManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling-plans:CreateScalingPlan",
        "autoscaling-plans:DeleteScalingPlan",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:DescribeScalingPlanResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridge",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CWAlarmManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ECSTagging",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "CWLogGroupManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
```

```
        "logs:DescribeLogGroups",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
    },
    {
      "Sid" : "CWLogStreamManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
    },
    {
      "Sid" : "ExecuteCommandSessionManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExecuteCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*",
        "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
      ]
    },
    {
      "Sid" : "OpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:CreateHttpNamespace",
        "servicediscovery:CreateService"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonECSManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CloudMapResourceTagging",
      "Effect" : "Allow",
      "Action" : "servicediscovery:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonECSManaged" : "*"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDeletion",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DeleteService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "CloudMapResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudMapResourceAttributeManagement",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:UpdateServiceAttributes"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonECSTaskExecutionRolePolicy

Descrizione: fornisce l'accesso ad altre risorse AWS di servizio necessarie per eseguire le attività di Amazon ECS

`AmazonECSTaskExecutionRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonECSTaskExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 16 novembre 2017, 18:48 UTC
- Ora modificata: 16 novembre 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
```

```
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEFSCSIDriverPolicy

Descrizione: Fornisce l'accesso di gestione alle risorse EFS e l'accesso in lettura a EC2

`AmazonEFSCSIDriverPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEFSCSIDriverPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 25 luglio 2023, 20:10 UTC
- Ora modificata: 25 luglio 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateAccessPoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowTagNewAccessPoints",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "elasticfilesystem:CreateAction" : "CreateAccessPoint"
        },
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowDeleteAccessPoint",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:DeleteAccessPoint",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKS_CNI_Policy

Descrizione: questa policy fornisce al plugin Amazon VPC CNI (amazon-vpc-cni-k8s) le autorizzazioni necessarie per modificare la configurazione dell'indirizzo IP sui nodi di lavoro EKS. Questo set di autorizzazioni consente al CNI di elencare, descrivere e modificare le interfacce di rete elastiche per tuo conto. Ulteriori informazioni sul plugin AWS VPC CNI sono disponibili qui: 8s https://github.com/aws/ amazon-vpc-cni-k

`AmazonEKS_CNI_Policy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonEKS_CNI_Policy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2018, 21:07 UTC
- Ora modificata: 4 marzo 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSCNIPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSBlockStoragePolicy

Descrizione: policy allegata all'EKS Cluster Role che concede le autorizzazioni per gestire le risorse di storage a blocchi del cluster.

`AmazonEKSBlockStoragePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSBlockStoragePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 30 ottobre 2024, 20:18 UTC
- Ora modificata: 30 ottobre 2024, 20:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
```

```
            "CreateSnapshot"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "kubernetes.io/created-for/*",
            "Name",
            "KubernetesCluster"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeSnapshotName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "Name"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSBlockStoragePolicyV2

Descrizione: policy allegata all'EKS Cluster Role che concede le autorizzazioni per gestire le risorse di storage a blocchi del cluster.

`AmazonEKSBlockStoragePolicyV2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSBlockStoragePolicyV2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2026, 16:27 UTC
- Ora modificata: 11 maggio 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicyV2`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "kubernetes.io/created-for/*",
            "Name",
            "KubernetesCluster"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeSnapshotName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "Name"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSClusterPolicy

Descrizione: questa policy fornisce a Kubernetes le autorizzazioni necessarie per gestire le risorse per tuo conto. Kubernetes richiede Ec2: CreateTags autorizzazioni per inserire informazioni identificative sulle risorse EC2, tra cui, a titolo esemplificativo, istanze, gruppi di sicurezza e interfacce di rete elastiche.

`AmazonEKSClusterPolicy`è una AWS politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSClusterPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2018, 21:06 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSClusterPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:UpdateAutoScalingGroup",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteRoute",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyVolume",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstanceTopology",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateListener",
```

```
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSClusterPolicySLRCreate",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonEKSClusterPolicyENIDelete",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "amazon-vpc-cni"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSComputePolicy

Descrizione: policy allegata all'EKS Cluster Role che concede le autorizzazioni per gestire le risorse di elaborazione del cluster.

`AmazonEKSComputePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSComputePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 novembre 2024, 21:46 UTC
- Ora modificata: 18 maggio 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSComputePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-node-class-name" : "*",
          "aws:RequestTag/eks:kubernetes-node-pool-name" : "*"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-node-class-name",
            "eks:kubernetes-node-pool-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DescribeCapacityReservations",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSConnectorServiceRolePolicy

Descrizione: questa policy consente ad Amazon EKS di gestire AWS le risorse per il connettore EKS

`AmazonEKSConnectorServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 04 settembre 2021, 20:31 UTC
- Ora modificata: 15 ottobre 2025, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation",
        "ssm:DescribeInstanceInformation",
        "ssm:DeleteActivation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectorAgentStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:ssm:*::document/AmazonEKS-ExecuteNonInteractiveCommand"
      ]
    },
    {
      "Sid" : "ConnectorAgentDeregister",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "PassAnyRoleToSsm",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutManagedEventRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.ssm"
        }
      }
    },
    {
      "Sid" : "PutManagedEventTarget",
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSDashboardConsoleReadOnly

Descrizione: fornisce l'accesso in sola lettura per visualizzare il pannello di controllo nella console Amazon EKS. La dashboard aggrega informazioni su più cluster e risorse correlate utilizzando Organizations AWS .

`AmazonEKSDashboardConsoleReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSDashboardConsoleReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 giugno 2025, 17:22 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSDashboardConsoleReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSDashboardReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListDashboardData",
        "eks:ListDashboardResources",
        "eks:DescribeClusterVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSDashboardServiceRolePolicy

Descrizione: questa policy consente a Amazon EKS Dashboard di accedere e visualizzare informazioni a livello di organizzazione. La policy consente al servizio EKS Dashboard di raccogliere informazioni sulla struttura e sugli account della vostra AWS Organizations.

`AmazonEKSDashboardServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 8 maggio 2025, 19:07 UTC
- Ora modificata: 08 maggio 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSDashboardServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSFargatePodExecutionRolePolicy

Descrizione: fornisce l'accesso ad altre risorse AWS di servizio necessarie per eseguire i pod Amazon EKS su AWS Fargate

`AmazonEKSFargatePodExecutionRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSFargatePodExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 novembre 2019, 04:34 UTC
- Ora modificata: 22 novembre 2019, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSForFargateServiceRolePolicy

Descrizione: questa politica concede le autorizzazioni necessarie ad Amazon EKS per eseguire attività fargate

`AmazonEKSForFargateServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 22 novembre 2019, 04:36 UTC

- Ora modificata: 22 novembre 2019, 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSLoadBalancingPolicy

Descrizione: policy allegata all'EKS Cluster Role che concede le autorizzazioni per gestire le risorse di bilanciamento del carico del cluster.

`AmazonEKSLoadBalancingPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSLoadBalancingPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 ottobre 2024, 20:18 UTC
- Ora modificata: 16 giugno 2026, 00:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLoadBalancingPolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateRule",
        "ec2:CreateSecurityGroup"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group-rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateTargetGroup",
            "CreateListener",
            "CreateRule"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:SetIpAddressType",
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:SetSubnets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:ModifyListenerAttributes",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:ModifyIpPools",
        "elasticloadbalancing:ModifyCapacityReservation",
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:TagResource"
      ],
      "Resource" : "arn:aws:shield::*:protection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPoolClient",
        "acm:ListCertificates",
        "acm:DescribeCertificate",
```

```
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:SetRulePriorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeIpamPools"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSLocalOutpostClusterPolicy

Descrizione: questa policy fornisce le autorizzazioni alle istanze del piano di controllo del cluster locale EKS in esecuzione nel tuo account per gestire le risorse per tuo conto.

`AmazonEKSLocalOutpostClusterPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSLocalOutpostClusterPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 agosto 2022, 21:56 UTC
- Ora modificata: 24 ottobre 2024, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeAvailabilityZones",
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:DescribeInstanceProperties",
        "ssm:DescribeDocumentParameters",
        "ssm:ListInstanceAssociations",
        "ssm:RegisterManagedInstance",
        "ssm:UpdateInstanceInformation",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:PutComplianceItems",
        "ssm:PutInventory",
        "ecr-public:GetAuthorizationToken",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
```

```
      "Resource" : [
        "arn:aws:ecr:*:*:repository/eks/*",
        "arn:aws:ecr:*:*:repository/bottlerocket-admin",
        "arn:aws:ecr:*:*:repository/bottlerocket-control-eks",
        "arn:aws:ecr:*:*:repository/diagnostics-collector-eks",
        "arn:aws:ecr:*:*:repository/kubelet-config-updater"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSLocalOutpostServiceRolePolicy

Descrizione: consente ad Amazon EKS Local di chiamare AWS i servizi per tuo conto.

`AmazonEKSLocalOutpostServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 23 agosto 2022, 21:53 UTC
- Ora modificata: 26 giugno 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribePlacementGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DeleteSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DescribeSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*::document/AmazonEKS-ControlPlaneInstanceProxy"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:ResumeSession",
        "ssm:TerminateSession"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSMCPReadOnlyAccess

Descrizione: fornisce accesso in sola lettura al servizio Amazon EKS MCP. Questa policy concede le autorizzazioni per utilizzare solo strumenti di sola lettura nel servizio EKS MCP destinati all'osservabilità, alla risoluzione dei problemi, al recupero di informazioni sulle risorse EKS e all'ottenimento di suggerimenti ottimizzati per EKS.

`AmazonEKSMCPReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSMCPReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2025, 17:19 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonEKSMCPReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListClusters",
        "eks:DescribeNodegroup",
        "eks:ListNodegroups",
        "eks:DescribeAddon",
        "eks:ListAddons",
        "eks:DescribeAccessEntry",
        "eks:ListAccessEntries",
        "eks:DescribeInsight",
        "eks:ListInsights",
        "eks:AccessKubernetesApi"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks-mcp:InvokeMcp",
        "eks-mcp:CallReadOnlyTool"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSNetworkingPolicy

Descrizione: Politica allegata all'EKS Cluster Role che concede le autorizzazioni per gestire le risorse di rete del cluster.

`AmazonEKSNetworkingPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSNetworkingPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 ottobre 2024, 22:34 UTC
- Ora modificata: 20 febbraio 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSNetworkingPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-cni-node-name" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-cni-node-name"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:ModifyNetworkInterfaceAttribute",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSServicePolicy

Descrizione: questa policy consente ad Amazon Elastic Container Service for Kubernetes di creare e gestire le risorse necessarie per gestire i cluster EKS.

`AmazonEKSServicePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSServicePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2018, 21:08 UTC
- Ora modificata: 14 ottobre 2024, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSServiceRolePolicy

Descrizione: un Service-Linked ruolo richiesto ad Amazon EKS per chiamare AWS i servizi per tuo conto.

`AmazonEKSServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 21 febbraio 2020, 20:10 UTC
- Ora modificata: 10 luglio 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Versione della politica

Versione della politica: v26 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "eks:DescribeCluster",
        "ec2:DescribeIpamPools",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeTrustStores",
        "elasticloadbalancing:DescribeCapacityReservation",
```

```
        "iam:ListAttachedRolePolicies",
        "pricing:GetProducts",
        "shield:GetSubscriptionState",
        "shield:DescribeProtection",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "cloudwatch:namespace" : "AWS/EKS"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry",
        "eks:DeleteAccessEntry"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "STANDARD"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : [
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputePolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputeClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingPolicy",
```

```
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSLoadBalancingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSLoadBalancingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSBlockStoragePolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSBlockStorageClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSHybridPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSEventPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSPodIdentityPolicy"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "eks:DescribeAccessEntry",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "EC2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/EKS*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.ec2",
```

```
            "aws.health"
          ]
        },
        "StringEquals" : {
          "events:ManagedBy" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "arn:aws:events:*:*:rule/EKS*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "arn:aws:iam::*:instance-profile/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSVPCResourceController

Descrizione: Policy utilizzata da VPC Resource Controller per gestire ENI e IPs per i nodi di lavoro.

`AmazonEKSVPCResourceController`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSVPCResourceController` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 agosto 2020, 00:55 UTC
- Ora modificata: 12 agosto 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "eks-vpc-resource-controller"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSWorkerNodeMinimalPolicy

Descrizione: questa policy consente ai nodi di lavoro Amazon EKS di connettersi ai cluster Amazon EKS.

`AmazonEKSWorkerNodeMinimalPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSWorkerNodeMinimalPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 ottobre 2024, 20:03 UTC
- Ora modificata: 02 ottobre 2024, 20:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEKSWorkerNodePolicy

Descrizione: questa policy consente ai nodi di lavoro Amazon EKS di connettersi ai cluster Amazon EKS.

`AmazonEKSWorkerNodePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEKSWorkerNodePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2018, 21:09 UTC
- Ora modificata: 27 novembre 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElastiCacheFullAccess

Descrizione: fornisce l'accesso completo ad Amazon ElastiCache tramite Console di gestione AWS.

`AmazonElastiCacheFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElastiCacheFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 28 novembre 2023, 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : "elasticache:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/elasticache.amazonaws.com/
AWSServiceRoleForElastiCache",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "elasticache.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpoints",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToEc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToAutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListLogDeliveryStreams",
      "Effect" : "Allow",
```

```
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToOutposts",
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElastiCacheReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon ElastiCache tramite Console di gestione AWS.

`AmazonElastiCacheReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElastiCacheReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticache:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticContainerRegistryPublicFullAccess

Descrizione: Fornisce accesso amministrativo alle risorse pubbliche di Amazon ECR

`AmazonElasticContainerRegistryPublicFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticContainerRegistryPublicFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 17:25 UTC
- Ora modificata: 01 dicembre 2020, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:*",
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticContainerRegistryPublicPowerUser

Descrizione: fornisce l'accesso completo agli archivi pubblici di Amazon ECR, ma non consente l'eliminazione degli archivi o la modifica delle policy.

`AmazonElasticContainerRegistryPublicPowerUser`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticContainerRegistryPublicPowerUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 01 dicembre 2020, 16:16 UTC
- Ora modificata: 01 dicembre 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:InitiateLayerUpload",
        "ecr-public:UploadLayerPart",
        "ecr-public:CompleteLayerUpload",
        "ecr-public:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticContainerRegistryPublicReadOnly

Descrizione: fornisce accesso in sola lettura ai repository pubblici di Amazon ECR.

`AmazonElasticContainerRegistryPublicReadOnly`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticContainerRegistryPublicReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 17:27 UTC
- Ora modificata: 01 dicembre 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticFileSystemClientFullAccess

Descrizione: fornisce l'accesso del client root a un file system Amazon EFS

`AmazonElasticFileSystemClientFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticFileSystemClientFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 gennaio 2020, 16:27 UTC
- Ora modificata: 13 gennaio 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticFileSystemClientReadOnlyAccess

Descrizione: fornisce l'accesso client di sola lettura a un file system Amazon EFS

`AmazonElasticFileSystemClientReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticFileSystemClientReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 gennaio 2020, 16:24 UTC
- Ora modificata: 13 gennaio 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:DescribeMountTargets"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticFileSystemClientReadWriteAccess

Descrizione: fornisce l'accesso client di lettura e scrittura a un file system Amazon EFS

`AmazonElasticFileSystemClientReadWriteAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticFileSystemClientReadWriteAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 gennaio 2020, 16:21 UTC
- Ora modificata: 13 gennaio 2020, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticFileSystemFullAccess

Descrizione: fornisce l'accesso completo ad Amazon EFS tramite Console di gestione AWS.

`AmazonElasticFileSystemFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticFileSystemFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2015, 16:22 UTC
- Ora modificata: 07 novembre 2024, 19:34 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:CreateAccessPoint",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "elasticfilesystem:DeleteTags",
        "elasticfilesystem:DeleteAccessPoint",
        "elasticfilesystem:DeleteFileSystemPolicy",
        "elasticfilesystem:DeleteReplicationConfiguration",
```

```
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ModifyMountTargetSecurityGroups",
        "elasticfilesystem:PutAccountPreferences",
        "elasticfilesystem:PutBackupPolicy",
        "elasticfilesystem:PutLifecycleConfiguration",
        "elasticfilesystem:PutFileSystemPolicy",
        "elasticfilesystem:UpdateFileSystem",
        "elasticfilesystem:UpdateFileSystemProtection",
        "elasticfilesystem:TagResource",
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:Backup",
        "elasticfilesystem:Restore",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEFS",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticfilesystem.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForEFS",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticfilesystem.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticFileSystemReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon EFS tramite Console di gestione AWS.

`AmazonElasticFileSystemReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticFileSystemReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2015, 16:25 UTC
- Ora modificata: 07 novembre 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:ReplicationRead",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticFileSystemServiceRolePolicy

Descrizione: consente ad Amazon Elastic File System di gestire AWS le risorse per tuo conto

`AmazonElasticFileSystemServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 5 novembre 2019, 16:52 UTC
- Ora modificata: 07 novembre 2024, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
      ],
      "Resource" : [
```

```
        "arn:aws:backup:*:*:backup-plan:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticFileSystemsUtils

Descrizione: consente ai clienti di utilizzare AWS Systems Manager per gestire automaticamente il pacchetto Amazon EFS utilities (amazon-efs-utils) sulle loro istanze EC2 e di utilizzarlo CloudWatchLog per ricevere notifiche di montaggio del file system EFS. success/failure

`AmazonElasticFileSystemsUtils`è una policy gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticFileSystemsUtils` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 settembre 2020, 15:16 UTC
- Ora modificata: 07 aprile 2026, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "efs-utils/S3Files",
            "efs-utils/EFS"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticMapReduceEditorsRole

Descrizione: policy predefinita per il ruolo di servizio Amazon Elastic MapReduce Editors.

`AmazonElasticMapReduceEditorsRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticMapReduceEditorsRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 16 novembre 2018, 21:55 UTC
- Ora modificata: 09 febbraio 2023, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:elasticmapreduce:editor-id",
            "aws:elasticmapreduce:job-flow-id"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticMapReduceforAutoScalingRole

Descrizione: Amazon Elastic MapReduce for Auto Scaling. Ruolo per consentire ad Auto Scaling di aggiungere e rimuovere istanze dal cluster EMR.

`AmazonElasticMapReduceforAutoScalingRole`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticMapReduceforAutoScalingRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 18 novembre 2016, 01:09 UTC
- Ora modificata: 18 novembre 2016, 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticMapReduceforEC2Role

Descrizione: policy predefinita per il ruolo di servizio Amazon Elastic MapReduce for EC2.

`AmazonElasticMapReduceforEC2Role`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticMapReduceforEC2Role` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 11 agosto 2017, 23:57 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "cloudwatch:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSteps",
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:MergeShards",
        "kinesis:PutRecord",
        "kinesis:SplitShard",
        "rds:Describe*",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*",
```

```
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:UpdatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:CreateUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:DeleteUserDefinedFunction",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticMapReduceFullAccess

Descrizione: questa politica si trova su un percorso obsoleto. Vedi la documentazione come guida: https://docs.aws.amazon.com/emr/ latest/ManagementGuide/emr - .html. managed-iam-policies

Fornisce accesso completo ad Amazon Elastic MapReduce e ai servizi sottostanti che richiede, come EC2 e S3

`AmazonElasticMapReduceFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticMapReduceFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 11 ottobre 2019, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
```

```
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:List*",
        "s3:*",
        "sdb:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
```

```
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticMapReducePlacementGroupPolicy

Descrizione: Politica per consentire a EMR di creare, descrivere ed eliminare i gruppi di collocamento EC2.

`AmazonElasticMapReducePlacementGroupPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticMapReducePlacementGroupPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 settembre 2020, 00:37 UTC
- Ora modificata: 29 settembre 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups"
      ]
    },
    {
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticMapReduceReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Elastic MapReduce tramite Console di gestione AWS.

`AmazonElasticMapReduceReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticMapReduceReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 29 luglio 2020, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sdb:Select",
        "cloudwatch:GetMetricStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticMapReduceRole

Descrizione: questa politica si trova su un percorso obsoleto. Vedi la documentazione come guida: https://docs.aws.amazon.com/emr/ latest/ManagementGuide/emr - .html. managed-iam-policies Policy predefinita per il ruolo del MapReduce servizio Amazon Elastic.

`AmazonElasticMapReduceRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticMapReduceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 24 giugno 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:PassRole",
        "s3:CreateBucket",
        "s3:Get*",
        "s3:List*",
        "sdb:BatchPutAttributes",
        "sdb:Select",
        "sqs:CreateQueue",
        "sqs:Delete*",
        "sqs:GetQueue*",
        "sqs:PurgeQueue",
        "sqs:ReceiveMessage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:Describe*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticsearchServiceRolePolicy

Descrizione: consenti ad Amazon Elasticsearch Service di accedere ad altri AWS servizi come le API di rete EC2 per tuo conto.

`AmazonElasticsearchServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 07 luglio 2017, 00:15 UTC
- Ora modificata: 22 giugno 2026, 12:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973135",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973136",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
```

```
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticTranscoder_FullAccess

Descrizione: concede agli utenti l'accesso completo a Elastic Transcoder e l'accesso ai servizi associati necessari per la funzionalità completa di Elastic Transcoder.

`AmazonElasticTranscoder_FullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticTranscoder_FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 aprile 2018, 18:59 UTC
- Ora modificata: 10 giugno 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "elastictranscoder.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticTranscoder_JobsSubmitter

Descrizione: concede agli utenti il permesso di modificare le preimpostazioni, inviare lavori e visualizzare le impostazioni di Elastic Transcoder. Questa politica concede inoltre un accesso in sola

lettura ad alcuni altri servizi necessari per utilizzare la console Elastic Transcode, tra cui S3, IAM e SNS.

`AmazonElasticTranscoder_JobsSubmitter`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticTranscoder_JobsSubmitter` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 giugno 2018, 21:12 UTC
- Ora modificata: 10 giugno 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "elastictranscoder:*Job",
        "elastictranscoder:*Preset",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
```

```
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticTranscoder_ReadOnlyAccess

Descrizione: concede agli utenti l'accesso in sola lettura a Elastic Transcoder e l'accesso agli elenchi ai servizi correlati.

`AmazonElasticTranscoder_ReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticTranscoder_ReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 07 giugno 2018, 21:09 UTC
- Ora modificata: 10 giugno 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonElasticTranscoderRole

Descrizione: policy predefinita per il ruolo del servizio Amazon Elastic Transcoder.

`AmazonElasticTranscoderRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonElasticTranscoderRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 13 giugno 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:Get*",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:*MultipartUpload*"
      ],
      "Sid" : "1",
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Sid" : "2",
```

```
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEMRCleanupPolicy

Descrizione: consente le azioni richieste da EMR per terminare ed eliminare le risorse AWS EC2 se il ruolo del servizio EMR ha perso tale capacità.

`AmazonEMRCleanupPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 settembre 2017, 23:54 UTC
- Ora modificata: 29 settembre 2020, 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DeleteLaunchTemplate",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:CancelSpotInstanceRequests",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:DeleteVolume",
        "ec2:DescribePlacementGroups",
        "ec2:DeletePlacementGroup"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEMRContainersServiceRolePolicy

Descrizione: consente l'accesso ad altre risorse di AWS servizio necessarie per eseguire Amazon EMR

`AmazonEMRContainersServiceRolePolicy`è una policy AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 09 dicembre 2020, 00:38 UTC
- Ora modificata: 24 luglio 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Versione della politica

Versione della politica: v6 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-containers:managed-endpoint-resource" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:ModifyVpcEndpointServicePermissions"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/emr-containers:managed-endpoint-resource" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpointServiceConfiguration"
        }
      }
    },
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/EMRContainers"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEMRFullAccessPolicy_v2

Descrizione: Fornisce accesso completo ad Amazon EMR

`AmazonEMRFullAccessPolicy_v2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEMRFullAccessPolicy_v2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 marzo 2021, 01:50 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:CreateEditor",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteEditor",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
```

```
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ModifyCluster",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:ModifyInstanceGroups",
        "elasticmapreduce:OpenEditorInConsole",
        "elasticmapreduce:PutAutoScalingPolicy",
        "elasticmapreduce:PutBlockPublicAccessConfiguration",
        "elasticmapreduce:PutManagedScalingPolicy",
        "elasticmapreduce:RemoveAutoScalingPolicy",
        "elasticmapreduce:RemoveManagedScalingPolicy",
        "elasticmapreduce:RemoveTags",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:StartEditor",
        "elasticmapreduce:StopEditor",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleForElasticMapReduce",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_DefaultRole_V2",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticmapreduce.amazonaws.com*"
        }
```

```
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticmapreduce.amazonaws.com*/AWSServiceRoleForEMRCleanup*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleUIActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEMRReadOnlyAccessPolicy_v2

Descrizione: fornisce accesso in sola lettura ad Amazon EMR e alle metriche associate CloudWatch .

`AmazonEMRReadOnlyAccessPolicy_v2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEMRReadOnlyAccessPolicy_v2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 marzo 2021, 01:39 UTC

- Ora modificata: 02 agosto 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEMRServerlessServiceRolePolicy

Descrizione: consente l'accesso ad altre risorse di AWS servizio necessarie per eseguire Amazon EMRServerless

`AmazonEMRServerlessServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 maggio 2022, 23:15 UTC
- Ora modificata: 25 gennaio 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2PolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/EMRServerless",
            "AWS/Usage"
          ]
```

```
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEMRServicePolicy_v2

Descrizione: questa policy viene utilizzata per il ruolo di servizio Amazon EMR e NON deve essere utilizzata per altri utenti o ruoli IAM nel tuo account. La politica concede le autorizzazioni per creare e gestire le risorse associate all'EMR e ai servizi correlati necessari per il funzionamento del cluster EMR.

`AmazonEMRServicePolicy_v2`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonEMRServicePolicy_v2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 marzo 2021, 01:11 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateWithEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedInstancesAndVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ResourcesToLaunchEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
```

```
    },
    {
      "Sid" : "ManageEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ManageTagsOnEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateTaggedEMRResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
      ]
    },
    {
      "Sid" : "ListActionsForEC2Resources",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
    },
    {
      "Sid" : "DeletePlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsForCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
    },
    {
      "Sid" : "PassRoleForAutoScaling",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "CreateAndModifyEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    },
    {
      "Sid" : "TagEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEMRServicePolicyForSessions

Descrizione: Fornisce le autorizzazioni per fornire e gestire Network Load Balancer, servizi endpoint VPC e gruppi di sicurezza necessari per le sessioni interattive di Amazon EMR Spark Connect su EMR su cluster EC2.

`AmazonEMRServicePolicyForSessions`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonEMRServicePolicyForSessions` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 giugno 2026, 19:57 UTC
- Ora modificata: 22 giugno 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicyForSessions`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NLBProvisioning",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
```

```
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "NLBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:SetSecurityGroups",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "NLBDescribes",
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCEndpointServiceProvisioning",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint-service/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:ModifyVpcEndpointServicePermissions"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceDescribes",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagOnCreateEndpointServiceResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpointServiceConfiguration"
          ]
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRoleForELB",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityGroupProvisioning",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupCreateInVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonESCognitoAccess

Descrizione: fornisce un accesso limitato al servizio di configurazione Amazon Cognito.

`AmazonESCognitoAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonESCognitoAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 febbraio 2018, 22:29 UTC
- Ora modificata: 20 dicembre 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonESFullAccess

Descrizione: fornisce l'accesso completo al servizio di configurazione Amazon ES.

`AmazonESFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonESFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 ottobre 2015, 19:14 UTC
- Ora modificata: 1 ottobre 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "es:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonESReadOnlyAccess

Descrizione: fornisce accesso in sola lettura al servizio di configurazione Amazon ES.

`AmazonESReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonESReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 ottobre 2015, 19:18 UTC
- Ora modificata: 03 ottobre 2018, 03:32 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "es:Describe*",
        "es:List*",
        "es:Get*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgeApiDestinationsServiceRolePolicy

Descrizione: consente di accedere EventBridge alle risorse di Secret Manager per tuo conto.

`AmazonEventBridgeApiDestinationsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 11 febbraio 2021, 20:52 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : [
            "arn:aws:secretsmanager:*:*:secret:events!connection/*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/EventBridgeApiDestinations" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgeFullAccess

Descrizione: fornisce l'accesso completo ad Amazon EventBridge.

`AmazonEventBridgeFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEventBridgeFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 luglio 2019, 14:08 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleAccessForEventBridge",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgePipesFullAccess

Descrizione: fornisce l'accesso completo ad Amazon EventBridge Pipes.

`AmazonEventBridgePipesFullAccess` è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEventBridgePipesFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 01 dicembre 2022, 17:03 UTC
- Ora modificata: 01 dicembre 2022, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgePipesActions",
      "Effect" : "Allow",
      "Action" : "pipes:*",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgePipesOperatorAccess

Descrizione: fornisce l'accesso in sola lettura e all'operatore (possibilità di interrompere e avviare Pipes) ad Amazon EventBridge Pipes.

`AmazonEventBridgePipesOperatorAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEventBridgePipesOperatorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2022, 17:04 UTC
- Ora modificata: 01 dicembre 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgePipesReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon EventBridge Pipes.

`AmazonEventBridgePipesReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEventBridgePipesReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2022, 17:04 UTC
- Ora modificata: 01 dicembre 2022, 17:04 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgeReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon EventBridge.

`AmazonEventBridgeReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEventBridgeReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 luglio 2019, 13:59 UTC
- Ora modificata: 01 dicembre 2022, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
```

```
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgeSchedulerFullAccess

Descrizione: la politica AmazonEventBridgeSchedulerFullAccess gestita concede le autorizzazioni per utilizzare tutte le azioni di EventBridge Scheduler per le pianificazioni e i gruppi di pianificazioni.

`AmazonEventBridgeSchedulerFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonEventBridgeSchedulerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 novembre 2022, 18:37 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgeSchedulerReadOnlyAccess

Descrizione: la politica AmazonEventBridgeSchedulerReadOnlyAccess gestita concede autorizzazioni di sola lettura per visualizzare i dettagli sulle pianificazioni e sui gruppi di pianificazioni

`AmazonEventBridgeSchedulerReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonEventBridgeSchedulerReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 novembre 2022, 18:50 UTC
- Ora modificata: 02 aprile 2026, 17:57 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:List*",
        "scheduler:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgeSchemasFullAccess

Descrizione: fornisce l'accesso completo ad Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEventBridgeSchemasFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2019, 23:12 UTC
- Ora modificata: 28 novembre 2019, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEventBridgeManageRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
```

```
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*Schemas*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgeSchemasReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonEventBridgeSchemasReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2019, 23:05 UTC
- Ora modificata: 01 maggio 2020, 00:50 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:ListDiscoverers",
        "schemas:DescribeDiscoverer",
        "schemas:ListRegistries",
        "schemas:DescribeRegistry",
        "schemas:SearchSchemas",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:DescribeSchema",
        "schemas:GetDiscoveredSchema",
        "schemas:DescribeCodeBinding",
        "schemas:GetCodeBindingSource",
        "schemas:ListTagsForResource",
        "schemas:GetResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEventBridgeSchemasServiceRolePolicy

Descrizione: concede le autorizzazioni per le Managed Rules create dagli schemi Amazon EventBridge .

`AmazonEventBridgeSchemasServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 27 novembre 2019, 01:10 UTC
- Ora modificata: 27 novembre 2019, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*Schemas-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonEVSServiceRolePolicy

Descrizione: concede a EVS le autorizzazioni per gestire le risorse per tuo conto

`AmazonEVSServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 16 maggio 2025, 23:37 UTC
- Ora modificata: 22 marzo 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEVSServiceRolePolicy`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ManageSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateEniWithTagStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "TagOnCreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AssignIpv6Addresses"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ManageInstanceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeInstanceAndVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "UpdateSecurityGroupStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "CloudWatchPutMetricDataStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/EVS"
          ]
        }
      }
    },
    {
      "Sid" : "AccessSecretStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/EvsAccess" : "false"
        }
      }
    },
    {
      "Sid" : "DecryptSecretWithKmsKeyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:*",
          "kms:EncryptionContext:SecretVersionId" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/EvsAccess" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeKmsKeyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/EvsAccess" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonFISServiceRolePolicy

Descrizione: Politica per consentire alla AWS FIS di gestire il monitoraggio e la selezione delle risorse per gli esperimenti.

`AmazonFISServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 dicembre 2020, 21:18 UTC
- Ora modificata: 25 ottobre 2022, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeDescribe",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Tagging",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeUserResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "iam:GetUser",
        "iam:GetRole",
        "iam:ListUsers",
        "iam:ListRoles",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "ecs:DescribeClusters",
        "ecs:DescribeTasks",
        "ecs:ListTasks",
        "eks:DescribeNodegroup",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonForecastFullAccess

Descrizione: Fornisce accesso a tutte le azioni per Amazon Forecast

`AmazonForecastFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonForecastFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 gennaio 2019, 01:52 UTC
- Ora modificata: 18 gennaio 2019, 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonFraudDetectorFullAccessPolicy

Descrizione: Fornisce accesso a tutte le azioni per Amazon Fraud Detector

`AmazonFraudDetectorFullAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonFraudDetectorFullAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 22:46 UTC
- Ora modificata: 03 dicembre 2019, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "frauddetector:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "frauddetector.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonFreeRTOSFullAccess

Descrizione: Policy di accesso completo per Amazon FreerTOS

`AmazonFreeRTOSFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonFreeRTOSFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 15:32 UTC
- Ora modificata: 29 novembre 2017, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "freertos:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonFreeRTOSOTAUpdate

Descrizione: consente all'utente di accedere ad Amazon FreerTOS OTA Update

`AmazonFreeRTOSOTAUpdate`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonFreeRTOSOTAUpdate` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 agosto 2018, 22:43 UTC
- Ora modificata: 18 dicembre 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::afr-ota*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "signer:StartSigningJob",
        "signer:DescribeSigningJob",
        "signer:GetSigningProfile",
        "signer:PutSigningProfile"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteJob",
        "iot:DescribeJob"
      ],
      "Resource" : "arn:aws:iot:*:*:job/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream"
      ],
      "Resource" : "arn:aws:iot:*:*:stream/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateStream",
        "iot:CreateJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonFSxConsoleFullAccess

Descrizione: fornisce l'accesso completo ad Amazon FSx e l'accesso ai AWS servizi correlati tramite Console di gestione AWS.

`AmazonFSxConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonFSxConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 16:36 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Versione della politica

Versione della politica: v20 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListResourcesAssociatedWithFSxFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "kms:ListAliases",
        "logs:DescribeLogGroups",
        "s3:ListBucket",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
```

```
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DetachAndDeleteS3AccessPoint",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateFSxSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonFSxConsoleReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon FSx e l'accesso ai AWS servizi correlati tramite Console di gestione AWS.

`AmazonFSxConsoleReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonFSxConsoleReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 16:35 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "kms:DescribeKey",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonFSxFullAccess

Descrizione: fornisce l'accesso completo ad Amazon FSx e l'accesso ai AWS servizi correlati.

`AmazonFSxFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonFSxFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 16:34 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDSDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
```

```
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DetachAndDeleteS3AccessPoint",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
```

```
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLRForFSx",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateLogsForFSxWindowsAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/fsx/*"
```

```
      ]
    },
    {
      "Sid" : "WriteToAmazonKinesisDataFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
      ]
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeEC2VpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonFSxReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon FSx.

`AmazonFSxReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonFSxReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 16:33 UTC
- Ora modificata: 28 novembre 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:Describe*",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonFSxServiceRolePolicy

Descrizione: consente FSx ad Amazon di gestire AWS le risorse per tuo conto

`AmazonFSxServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 28 novembre 2018, 10:38 UTC
- Ora modificata: 22 luglio 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
```

```
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/FSx"
        }
      }
    },
    {
      "Sid" : "TagResourceNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonFSx.FileSystemId"
        }
      }
    },
    {
      "Sid" : "ManageNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
        }
      }
    },
    {
      "Sid" : "ManageRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2:DeleteRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
```

```
      "Sid" : "PutCloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
    },
    {
      "Sid" : "ManageAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGlacierFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Glacier tramite. Console di gestione AWS

`AmazonGlacierFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonGlacierFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "glacier:*",
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGlacierReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Glacier tramite. Console di gestione AWS

`AmazonGlacierReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonGlacierReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 5 maggio 2016, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetJobOutput",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:GetVaultNotifications",
        "glacier:ListJobs",
        "glacier:ListMultipartUploads",
        "glacier:ListParts",
        "glacier:ListTagsForVault",
        "glacier:ListVaults"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGrafanaAthenaAccess

Descrizione: questa politica consente l'accesso ad Amazon Athena e alle dipendenze necessarie per abilitare l'interrogazione e la scrittura dei risultati su s3 dal plug-in Amazon Athena in Amazon Grafana.

`AmazonGrafanaAthenaAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonGrafanaAthenaAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 novembre 2021, 17:11 UTC
- Ora modificata: 22 novembre 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetWorkGroup",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::grafana-athena-query-results-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGrafanaCloudWatchAccess

Descrizione: questa politica garantisce l'accesso ad Amazon CloudWatch e alle dipendenze necessarie per l'uso CloudWatch come origine dati all'interno di Amazon Managed Grafana.

`AmazonGrafanaCloudWatchAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonGrafanaCloudWatchAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 marzo 2023, 22:41 UTC
- Ora modificata: 24 marzo 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
```

```
        "cloudwatch:GetInsightRuleReport"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:GetLogGroupFields",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:GetLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks",
        "oam:ListAttachedLinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGrafanaRedshiftAccess

Descrizione: questa policy garantisce l'accesso mirato ad Amazon Redshift e alle dipendenze necessarie per utilizzare il plug-in Amazon Redshift in Amazon Grafana.

`AmazonGrafanaRedshiftAccess`AWS è una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonGrafanaRedshiftAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 novembre 2021, 23:15 UTC
- Ora modificata: 26 novembre 2021, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "false"
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGrafanaServiceLinkedRolePolicy

Descrizione: fornisce l'accesso alle AWS risorse gestite o utilizzate da Amazon Grafana.

`AmazonGrafanaServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 08 novembre 2022, 23:10 UTC
- Ora modificata: 08 novembre 2022, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonGrafanaManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AmazonGrafanaManaged" : "false"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AmazonGrafanaManaged" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGuardDutyFullAccess

Descrizione: fornisce l'accesso completo all'uso di Amazon GuardDuty.

`AmazonGuardDutyFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonGuardDutyFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2017, 22:31 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamGetRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGuardDutyFullAccess_v2

Descrizione: Fornisce l'accesso completo all'uso di Amazon GuardDuty

`AmazonGuardDutyFullAccess_v2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonGuardDutyFullAccess_v2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 giugno 2025, 20:22 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess_v2`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyFullAccess",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGuardDutyServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
```

```
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyOrganizationsAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyIamRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
```

```
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGuardDutyMalwareProtectionServiceRolePolicy

Descrizione: la protezione GuardDuty da malware utilizza il ruolo collegato al servizio (SLR) denominato. AWSServiceRoleForAmazonGuardDutyMalwareProtection Questo ruolo collegato al servizio consente alla protezione GuardDuty da malware di eseguire scansioni senza agente per rilevare il malware. Consente di GuardDuty creare istantanee nell'account e condividerle con l'account del servizio per individuare eventuali malware. GuardDuty Valuta queste istantanee condivise e include i metadati delle istanze EC2 recuperati nei risultati di Malware Protection. GuardDuty Il ruolo AWSService RoleForAmazonGuardDutyMalwareProtection collegato al servizio si fida del servizio malware-protection.guardduty.amazonaws.com per l'assunzione del ruolo.

`AmazonGuardDutyMalwareProtectionServiceRolePolicy`è AWS una politica gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 luglio 2022, 19:06 UTC
- Ora modificata: 25 gennaio 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CreateSnapshotVolumeConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyScanId"
        }
      }
    },
    {
      "Sid" : "CreateTagsPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    },
    {
      "Sid" : "AddTagsToSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "GuardDutyExcluded",
            "GuardDutyFindingDetected"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteAndShareSnapshotPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "PreventPublicAccessToSnapshotPermission",
      "Effect" : "Deny",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/group" : "all"
        }
      }
    },
    {
      "Sid" : "CreateGrantPermission",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeKeyPermission",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
```

```
    {
      "Sid" : "GuardDutyLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
    {
      "Sid" : "GuardDutyLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
    },
    {
      "Sid" : "EBSDirectAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGuardDutyReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle GuardDuty risorse Amazon

`AmazonGuardDutyReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonGuardDutyReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2017, 22:29 UTC
- Ora modificata: 16 novembre 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonGuardDutyServiceRolePolicy

Descrizione: Abilita l'accesso alle AWS risorse utilizzate o gestite da Amazon Guard Duty

`AmazonGuardDutyServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 28 novembre 2017, 20:12 UTC

- Ora modificata: 24 aprile 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
```

```
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyCreateSLRPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        },
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.guardduty-data",
            "com.amazonaws.*.guardduty-data-fips"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutySecurityGroupManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
```

```
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/GuardDutyManaged" : "*"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateEksAddonPolicy",
      "Effect" : "Allow",
```

```
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEksAddonManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
    },
    {
      "Sid" : "GuardDutyEksClusterTagResourcePolicy",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
      "Effect" : "Allow",
      "Action" : "ecs:PutAccountSettingDefault",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:account-setting" : [
            "guardDutyActivate"
          ]
        }
      }
    },
    {
      "Sid" : "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:DeleteAssociation",
        "ssm:UpdateAssociation",
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmAddTagsToResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyManaged"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmCreateUpdateAssociationInstanceDocumentPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
    },
    {
```

```
      "Sid" : "SsmSendCommandPermission",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin"
      ]
    },
    {
      "Sid" : "SsmGetCommandStatus",
      "Effect" : "Allow",
      "Action" : "ssm:GetCommandInvocation",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudTrailCreateServiceLinkedChannelSid",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/guardduty/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonHealthLakeFullAccess

Descrizione: fornisce l'accesso completo al HealthLake servizio Amazon.

`AmazonHealthLakeFullAccess` è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonHealthLakeFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 febbraio 2021, 01:07 UTC
- Ora modificata: 17 febbraio 2021, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "healthlake.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonHealthLakeReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura al HealthLake servizio Amazon.

`AmazonHealthLakeReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonHealthLakeReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 febbraio 2021, 02:43 UTC
- Ora modificata: 17 febbraio 2021, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:ListFHIRDatastores",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:GetCapabilities",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonHoneycodeFullAccess

Descrizione: fornisce l'accesso completo a Honeycode tramite Console di gestione AWS e l'SDK.

`AmazonHoneycodeFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonHoneycodeFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 20:28 UTC
- Ora modificata: 24 giugno 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonHoneycodeReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a Honeycode tramite Console di gestione AWS e l'SDK.

`AmazonHoneycodeReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonHoneycodeReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 20:28 UTC
- Ora modificata: 01 dicembre 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:List*",
        "honeycode:Get*",
        "honeycode:Describe*",
        "honeycode:Query*"
```

```
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonHoneycodeServiceRolePolicy

Descrizione: è necessario un ruolo collegato al servizio per consentire ad Amazon Honeycode di accedere alle tue risorse.

`AmazonHoneycodeServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 novembre 2020, 18:03 UTC
- Ora modificata: 18 novembre 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonHoneycodeTeamAssociationFullAccess

Descrizione: fornisce l'accesso completo a Honeycode Team Association tramite Console di gestione AWS e l'SDK.

`AmazonHoneycodeTeamAssociationFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonHoneycodeTeamAssociationFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 24 giugno 2020, 20:28 UTC
- Ora modificata: 24 giugno 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations",
        "honeycode:ApproveTeamAssociation",
        "honeycode:RejectTeamAssociation"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonHoneycodeTeamAssociationReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a Honeycode Team Association tramite Console di gestione AWS e l'SDK.

`AmazonHoneycodeTeamAssociationReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonHoneycodeTeamAssociationReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 20:27 UTC
- Ora modificata: 24 giugno 2020, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonHoneycodeWorkbookFullAccess

Descrizione: fornisce l'accesso completo a Honeycode Workbook tramite Console di gestione AWS e l'SDK.

`AmazonHoneycodeWorkbookFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonHoneycodeWorkbookFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 20:28 UTC
- Ora modificata: 01 dicembre 2020, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:InvokeScreenAutomation",
        "honeycode:BatchCreateTableRows",
        "honeycode:BatchDeleteTableRows",
        "honeycode:BatchUpdateTableRows",
        "honeycode:BatchUpsertTableRows",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows",
        "honeycode:StartTableDataImportJob"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonHoneycodeWorkbookReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a Honeycode Workbook tramite Console di gestione AWS e l'SDK.

`AmazonHoneycodeWorkbookReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonHoneycodeWorkbookReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 20:28 UTC
- Ora modificata: 01 dicembre 2020, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspector2AgentlessServiceRolePolicy

Descrizione: concede ad Amazon Inspector l'accesso alle valutazioni di sicurezza necessarie Servizi AWS per eseguire valutazioni di sicurezza senza agenti

`AmazonInspector2AgentlessServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 novembre 2023, 15:18 UTC
- Ora modificata: 20 novembre 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstanceIdentification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAnyInstanceOrVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "DenyCreateSnapshotsOnExcludedInstances",
      "Effect" : "Deny",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsOnAnySnapshotOnlyWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "CreateSnapshots"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "DeleteOnlySnapshotsTaggedForScanning",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
```

```
          "ec2:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "DenyKmsDecryptForExcludedKeys",
      "Effect" : "Deny",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "vol-*"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        }
      }
```

```
    },
    {
      "Sid" : "DescribeKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListKeyResourceTags",
      "Effect" : "Allow",
      "Action" : "kms:ListResourceTags",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspector2AmiScanServiceRolePolicy

Descrizione: concede ad Amazon Inspector l'accesso ai dati Servizi AWS necessari per eseguire le valutazioni di sicurezza per AMI

`AmazonInspector2AmiScanServiceRolePolicy`è una policy gestita AWS .

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 30 luglio 2026, 17:57 UTC
- Ora modificata: 30 luglio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AmiScanServiceRolePolicy`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
    },
    {
      "Sid" : "AllowInspectorEnablementForAwsOrgPolicy",
      "Effect" : "Allow",
      "Action" : [
```

```
        "inspector2:AssociateMember",
        "inspector2:Disable",
        "inspector2:Enable",
        "inspector2:EnableDelegatedAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceGetAwsOrg",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceDelegatedAdminFromAwsOrg",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "ami.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmiIdentification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Sid" : "DenyGetSnapshotDataOnExcludedSnapshots",
      "Effect" : "Deny",
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DenyKmsDecryptForExcludedKeys",
      "Effect" : "Deny",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "vol-*",
```

```
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*",
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListKeyResourceTags",
      "Effect" : "Allow",
      "Action" : "kms:ListResourceTags",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspector2FullAccess

Descrizione: fornisce l'accesso completo ad Amazon Inspector e l'accesso ad altri servizi correlati, come le organizzazioni.

`AmazonInspector2FullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonInspector2FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 19:10 UTC
- Ora modificata: 25 aprile 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
```

```
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspector2FullAccess_v2

Descrizione: fornisce l'accesso completo ad Amazon Inspector e l'accesso ad altri servizi correlati, come le organizzazioni con accesso organizzativo restrittivo.

`AmazonInspector2FullAccess_v2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonInspector2FullAccess_v2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 luglio 2025, 16:07 UTC
- Ora modificata: 08 luglio 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess_v2`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com",
            "thirdparty.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowServicePrincipalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "inspector2.amazonaws.com",
```

```
            "agentless.inspector2.amazonaws.com",
            "thirdparty.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOrganizationalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid" : "AllowAccountsBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowConfigConnectorWriteAndList",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConnector",
        "config:ListConnectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigConnectorRead",
      "Effect" : "Allow",
      "Action" : "config:GetConnector",
      "Resource" : "arn:aws:config:*:*:connector/*"
    },
    {
      "Sid" : "AllowCreateConfigThirdPartySLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "thirdparty.config.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspector2ManagedCisPolicy

Descrizione: si tratta di una politica gestita che il cliente deve associare ai propri ruoli per comunicare con il servizio di ispezione per le scansioni CIS

`AmazonInspector2ManagedCisPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonInspector2ManagedCisPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 gennaio 2024, 16:31 UTC
- Ora modificata: 24 gennaio 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspector2ManagedTelemetryPolicy

Descrizione: concede le autorizzazioni per comunicare con Inspector2 Telemetry Channel

`AmazonInspector2ManagedTelemetryPolicy`è AWS una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonInspector2ManagedTelemetryPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 febbraio 2026, 17:12 UTC
- Ora modificata: 13 febbraio 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedTelemetryPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForInspector2Telemetry",
      "Effect" : "Allow",
      "Action" : [
        "inspector2-telemetry:StartSession",
        "inspector2-telemetry:StopSession",
        "inspector2-telemetry:SendTelemetry",
        "inspector2-telemetry:NotifyHeartbeat"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspector2ReadOnlyAccess

Descrizione: fornisce accesso in sola lettura al servizio Amazon inspector2 e ai servizi di supporto pertinenti

`AmazonInspector2ReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonInspector2ReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 gennaio 2022, 14:45 UTC
- Ora modificata: 07 luglio 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "inspector2:BatchGet*",
        "inspector2:List*",
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:Search*",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowCrossServiceReadsForConnectorHealth",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:ListConfigurationRecorders",
        "config:GetConnector",
        "config:ListConnectors",
        "ssm:GetCloudConnector",
        "ssm:ListCloudConnectors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspector2ServiceRolePolicy

Descrizione: concede ad Amazon Inspector l'accesso ai dati necessari Servizi AWS per eseguire le valutazioni di sicurezza

`AmazonInspector2ServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 16 novembre 2021, 20:27 UTC

- Ora modificata: 16 giugno 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Versione della politica

Versione della politica: v27 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "PackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:ListImages",
        "ecr:PutRegistryScanningConfiguration",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "ssm:DescribeAssociation",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:ListAssociations",
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunction",
        "lambda:GetLayerVersion",
        "lambda:ListTags",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GatherInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce",
        "ssm:UpdateAssociation"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "GatherInventoryDeleteAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "DataSyncCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
      ]
    },
    {
      "Sid" : "ManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
```

```
    },
    {
      "Sid" : "LambdaCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetAccountConfiguration",
        "codeguru-security:GetFindings",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:DeleteScansByCategory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CodeGuruCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedRolePolicies",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "codeguru-security.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2DeepInspection",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:GetParameters",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-
paths"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListServiceLinkedChannels",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AllowToRunInvokeCisSpecificDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
      ]
    },
    {
      "Sid" : "AllowToRunCisCommandsToSpecificResources",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToPutCloudwatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Inspector2"
        }
      }
    },
```

```
    {
      "Sid" : "AllowListAccessToECSAndEKS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters",
        "ecs:ListTasks",
        "eks:ListClusters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAccessToECSTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowInspectorEnablementForAwsOrgPolicy",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:AssociateMember"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceDelegatedAdminFromAwsOrg",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspector2ThirdPartyServiceRolePolicy

Descrizione: concede le autorizzazioni ad Amazon Inspector per eseguire azioni per tuo conto per la scansione di risorse multi-cloud.

`AmazonInspector2ThirdPartyServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 26 giugno 2026, 15:27 UTC
- Ora modificata: 26 giugno 2026, 15:27 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ThirdPartyServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MultiCloudResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Search"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:view/ServiceViewForInspector*/
service-view"
    },
    {
      "Sid" : "MultiCloudStreamingAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateStreamingAccessForService",
        "resource-explorer-2:ListStreamingAccessForServices",
        "resource-explorer-2:DeleteStreamingAccessForService"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MultiCloudSsmAssociationWrite",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
```

```
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "MultiCloudSsmAssociationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*"
    },
    {
      "Sid" : "MultiCloudSsmAssociationList",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListAssociations",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeAssociationExecutionTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MultiCloudSsmGetDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MultiCloudSsmAutomation",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Sid" : "MultiCloudCloudConnectorManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateCloudConnector",
        "ssm:UpdateCloudConnector",
        "ssm:DeleteCloudConnector",
        "ssm:GetCloudConnector",
        "ssm:ListCloudConnectors",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:cloud-connector/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MultiCloudSsmPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/Inspector2SSMFederationRole*",
        "arn:aws:iam::*:role/Inspector2SSMDispatchRole*",
        "arn:aws:iam::*:role/Inspector2SSMAssumeRole*",
        "arn:aws:iam::*:role/Inspector2VmScannerRole*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MultiCloudIamGetRole",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/Inspector2SSMFederationRole*",
        "arn:aws:iam::*:role/Inspector2SSMDispatchRole*",
        "arn:aws:iam::*:role/Inspector2SSMAssumeRole*",
        "arn:aws:iam::*:role/Inspector2VmScannerRole*"
      ]
    },
    {
      "Sid" : "MultiCloudConfigSLRecWrite",
      "Effect" : "Allow",
      "Action" : [
        "config:PutThirdPartyServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MultiCloudConfigConnectorRead",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders",
        "config:GetConnector"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MultiCloudConfigMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetWebIdentityToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "sts:IdentityTokenAudience" : "false"
        },
        "ForAnyValue:StringLike" : {
          "sts:IdentityTokenAudience" : [
            "api://AzureADTokenExchange"
          ]
        }
      }
    },
    {
      "Sid" : "MultiCloudSsmSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspectorFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Inspector.

`AmazonInspectorFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonInspectorFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 ottobre 2015, 17:08 UTC
- Ora modificata: 21 dicembre 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "inspector.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/
AWSServiceRoleForAmazonInspector",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "inspector.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspectorReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Inspector.

`AmazonInspectorReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonInspectorReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 ottobre 2015, 17:08 UTC
- Ora modificata: 1 ottobre 2019, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonInspectorServiceRolePolicy

Descrizione: concede ad Amazon Inspector l'accesso ai dati necessari Servizi AWS per eseguire le valutazioni di sicurezza

`AmazonInspectorServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 novembre 2017, 15:48 UTC
- Ora modificata: 11 settembre 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "directconnect:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayVpcAttachments",
```

```
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKendraFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Kendra tramite. Console di gestione AWS

`AmazonKendraFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonKendraFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 16:15 UTC
- Ora modificata: 03 dicembre 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kendra.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
```

```
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonKendra-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kendra:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKendraReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon Kendra tramite. Console di gestione AWS

`AmazonKendraReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonKendraReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 16:13 UTC
- Ora modificata: 27 maggio 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kendra:Describe*",
        "kendra:List*",
        "kendra:Query",
        "kendra:GetQuerySuggestions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKeyspacesFullAccess

Descrizione: Fornisci l'accesso completo ad Amazon Keyspaces

`AmazonKeyspacesFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonKeyspacesFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 aprile 2020, 17:06 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CassandraFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesReplicationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesCDCServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra-
streams.amazonaws.com/AWSServiceRoleForAmazonKeyspacesCDC",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra-streams.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "Ec2VpcReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKeyspacesReadOnlyAccess

Descrizione: Fornisci accesso in sola lettura ad Amazon Keyspaces

`AmazonKeyspacesReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonKeyspacesReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 aprile 2020, 17:07 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKeyspacesReadOnlyAccess_v2

Descrizione: Fornisci accesso in sola lettura ad Amazon Keyspaces e ai servizi correlati AWS .

`AmazonKeyspacesReadOnlyAccess_v2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonKeyspacesReadOnlyAccess_v2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 settembre 2023, 17:01 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKinesisAnalyticsFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Kinesis Analytics tramite Console di gestione AWS.

`AmazonKinesisAnalyticsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonKinesisAnalyticsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 settembre 2016, 19:01 UTC
- Ora modificata: 21 settembre 2016, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisanalytics:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
```

```
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/kinesis-analytics*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKinesisAnalyticsReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon Kinesis Analytics tramite. Console di gestione AWS

`AmazonKinesisAnalyticsReadOnly`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonKinesisAnalyticsReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 settembre 2016, 18:16 UTC
- Ora modificata: 21 settembre 2016, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKinesisFirehoseFullAccess

Descrizione: fornisce l'accesso completo a tutti gli Amazon Kinesis Firehose Delivery Streams.

`AmazonKinesisFirehoseFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonKinesisFirehoseFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 ottobre 2015, 18:45 UTC
- Ora modificata: 7 ottobre 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKinesisFirehoseReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutti gli Amazon Kinesis Firehose Delivery Streams.

`AmazonKinesisFirehoseReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonKinesisFirehoseReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 7 ottobre 2015, 18:43 UTC
- Ora modificata: 7 ottobre 2015, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:Describe*",
        "firehose:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKinesisFullAccess

Descrizione: fornisce l'accesso completo a tutti gli stream tramite. Console di gestione AWS

`AmazonKinesisFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonKinesisFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesis:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKinesisReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutti gli stream tramite. Console di gestione AWS

`AmazonKinesisReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonKinesisReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:Get*",
        "kinesis:List*",
        "kinesis:Describe*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKinesisVideoStreamsFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Kinesis Video Console di gestione AWS Streams tramite.

`AmazonKinesisVideoStreamsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonKinesisVideoStreamsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2017, 23:27 UTC
- Ora modificata: 01 dicembre 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisvideo:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonKinesisVideoStreamsReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura a AWS Kinesis Video Console di gestione AWS Streams tramite.

`AmazonKinesisVideoStreamsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonKinesisVideoStreamsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2017, 23:14 UTC
- Ora modificata: 01 dicembre 2017, 23:14 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLaunchWizard_Fullaccess

Descrizione: accesso completo alla procedura guidata di AWS avvio e ad altri servizi richiesti.

`AmazonLaunchWizard_Fullaccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonLaunchWizard_Fullaccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 agosto 2020, 17:47 UTC
- Ora modificata: 22 febbraio 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
```

```
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:DeletePlacementGroup",
        "ec2:CreatePlacementGroup",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
```

```
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLog*",
        "logs:PutLogEvents",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*",
        "arn:aws:logs:*:*:log-group:*:*:*",
```

```
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogStream",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
```

```
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "logs:CreateLogGroup",
        "logs:GetLogDelivery",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLog*",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
```

```
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
```

```
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "ssm:DeleteOpsMetadata",
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource",
        "logs:UntagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:LaunchWizard*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLaunchWizardFullAccessV2

Descrizione: accesso completo alla procedura guidata di AWS avvio e ad altri servizi richiesti.

`AmazonLaunchWizardFullAccessV2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonLaunchWizardFullAccessV2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 settembre 2023, 17:14 UTC
- Ora modificata: 01 settembre 2023, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppInsightsActions0",
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupActions0",
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Sid" : "Route53Actions0",
      "Effect" : "Allow",
      "Action" : [
```

```
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions0",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsActions0",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Actions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
```

```
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Actions1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
```

```
        "ec2:AssociateVpcCidrBlock",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:DeletePlacementGroup",
        "ec2:CreatePlacementGroup",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "CloudFormationActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
    },
    {
      "Sid" : "Ec2Actions2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "IamActions0",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
```

```
    {
      "Sid" : "IamActions1",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AutoScalingActions0",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
```

```
        "arn:aws:sns:*:*:*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Sid" : "SsmActions1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "SsmActions2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
```

```
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions3",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
```

```
        "tag:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Sid" : "IamActions2",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "LaunchWizardActions0",
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SqsActions0",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Sid" : "CloudWatchActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Sid" : "EfsActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
```

```
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Sid" : "CloudFormationActions2",
      "Effect" : "Allow",
      "Action" : "cloudformation:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Sid" : "LambdaActions0",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
```

```
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Sid" : "DynamodbActions0",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions0",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions5",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions6",
      "Effect" : "Allow",
      "Action" : "ssm:DeleteOpsMetadata",
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Sid" : "SnsActions0",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Sid" : "FsxActions0",
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
      }
    },
    {
      "Sid" : "FsxActions1",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystem"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions2",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceCatalogActions0",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmActions7",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EfsActions1",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions0",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DescribeLogStreams",
        "logs:UntagResource",
        "logs:TagResource",
        "logs:CreateLogGroup",
        "logs:DeleteLogStream",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
```

```
        "logs:ListLogDeliveries"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*:log-stream:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions1",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FsxActions3",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "FsxActions4",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions5",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLexChannelsAccess

Descrizione: Questa politica consente ai clienti di chiamare Lex runtime dai canali

`AmazonLexChannelsAccess`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 13 gennaio 2021, 20:12 UTC
- Ora modificata: 13 gennaio 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "lex:ListBots"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLexFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Lex tramite Console di gestione AWS. Fornisce inoltre l'accesso per creare Lex Service Linked Roles e concedere le autorizzazioni Lex per richiamare un set limitato di funzioni Lambda.

`AmazonLexFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonLexFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 aprile 2017, 23:20 UTC
- Ora modificata: 16 aprile 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
```

```
          "lambda:Principal" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement4",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement5",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement6",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement7",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonLexFullAccessStatement8",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "replication.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement9",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lex.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement12",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "channels.lexv2.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AmazonLexFullAccessStatement13",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLexReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon Lex.

`AmazonLexReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonLexReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 aprile 2017, 23:13 UTC
- Ora modificata: 13 maggio 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexReadOnlyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "lex:GetBots",
        "lex:GetBotChannelAssociation",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
```

```
        "lex:GetUtterancesView",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotRecommendation",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:ListBots",
        "lex:ListBotLocales",
        "lex:ListBotAliases",
        "lex:ListBotAliasReplicas",
        "lex:ListBotChannels",
        "lex:ListBotRecommendations",
        "lex:ListBotReplicas",
        "lex:ListBotVersions",
        "lex:ListBotVersionReplicas",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListRecommendedIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "lex:SearchAssociatedTranscripts",
        "lex:ListCustomVocabularyItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLexReplicationPolicy

Descrizione: consente ad Amazon Lex di replicare le risorse Lex tra regioni per tuo conto.

`AmazonLexReplicationPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 31 gennaio 2024, 23:29 UTC
- Ora modificata: 24 giugno 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex:DeleteBotAlias",
        "lex:DescribeBotAlias",
        "lex:CreateBotVersion",
        "lex:DeleteBotVersion",
        "lex:DescribeBotVersion",
        "lex:CreateExport",
        "lex:DescribeBot",
        "lex:UpdateExport",
        "lex:DescribeExport",
        "lex:DescribeBotLocale",
        "lex:DescribeIntent",
        "lex:ListIntents",
        "lex:DescribeSlotType",
        "lex:ListSlotTypes",
        "lex:DescribeSlot",
        "lex:ListSlots",
        "lex:DescribeCustomVocabulary",
        "lex:StartImport",
        "lex:DescribeImport",
        "lex:CreateBot",
        "lex:UpdateBot",
        "lex:DeleteBot",
        "lex:CreateBotLocale",
        "lex:UpdateBotLocale",
        "lex:DeleteBotLocale",
        "lex:CreateIntent",
        "lex:UpdateIntent",
        "lex:DeleteIntent",
        "lex:CreateSlotType",
        "lex:UpdateSlotType",
        "lex:DeleteSlotType",
        "lex:CreateSlot",
        "lex:UpdateSlot",
        "lex:DeleteSlot",
        "lex:CreateCustomVocabulary",
        "lex:UpdateCustomVocabulary",
        "lex:DeleteCustomVocabulary",
        "lex:DeleteBotChannel",
        "lex:ListTagsForResource",
```

```
        "lex:TagResource",
        "lex:UntagResource",
        "lex:CreateResourcePolicy",
        "lex:DeleteResourcePolicy",
        "lex:DescribeResourcePolicy",
        "lex:UpdateResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:lex:*:*:bot/*",
        "arn:aws:lex:*:*:bot-alias/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lex:CreateUploadUrl",
        "lex:ListBots"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lexv2.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLexRunBotsOnly

Descrizione: fornisce l'accesso ad Amazon Lex conversazionale APIs.

`AmazonLexRunBotsOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonLexRunBotsOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 aprile 2017, 23:06 UTC
- Ora modificata: 18 agosto 2021, 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:PostContent",
        "lex:PostText",
        "lex:PutSession",
        "lex:GetSession",
        "lex:DeleteSession",
        "lex:RecognizeText",
        "lex:RecognizeUtterance",
        "lex:StartConversation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLexV2BotPolicy

Descrizione: Fornisce ai bot Lex V2 l'accesso per chiamare altri AWS servizi per tuo conto.

`AmazonLexV2BotPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 13 gennaio 2021, 20:10 UTC

- Ora modificata: 13 gennaio 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLookoutEquipmentFullAccess

Descrizione: Fornisce accesso completo alle operazioni di Amazon Lookout for Equipment

`AmazonLookoutEquipmentFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonLookoutEquipmentFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 8 aprile 2021, 15:52 UTC
- Ora modificata: 24 novembre 2021, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "lookoutequipment.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "lookoutequipment.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLookoutEquipmentReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura ad Amazon Lookout for Equipments

`AmazonLookoutEquipmentReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonLookoutEquipmentReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 maggio 2021, 16:47 UTC
- Ora modificata: 10 novembre 2022, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:Describe*",
        "lookoutequipment:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLookoutMetricsFullAccess

Descrizione: Fornisce accesso a tutte le azioni per Amazon Lookout for Metrics

`AmazonLookoutMetricsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonLookoutMetricsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 07 maggio 2021, 00:43 UTC
- Ora modificata: 07 maggio 2021, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "lookoutmetrics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*LookoutMetrics*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lookoutmetrics.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLookoutMetricsReadOnlyAccess

Descrizione: dà accesso a tutte le azioni di sola lettura per Amazon Lookout for Metrics

`AmazonLookoutMetricsReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonLookoutMetricsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Tempo di creazione: 07 maggio 2021, 00:43 UTC
- Ora modificata: 04 gennaio 2022, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:DescribeMetricSet",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:DescribeAnomalyDetectionExecutions",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListTagsForResource",
        "lookoutmetrics:ListAnomalyGroupSummaries",
        "lookoutmetrics:ListAnomalyGroupTimeSeries",
        "lookoutmetrics:ListAnomalyGroupRelatedMetrics",
        "lookoutmetrics:GetAnomalyGroup",
        "lookoutmetrics:GetDataQualityMetrics",
        "lookoutmetrics:GetSampleData",
        "lookoutmetrics:GetFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLookoutVisionConsoleFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Lookout for Vision e l'accesso mirato al servizio richiesto e alle dipendenze della console.

`AmazonLookoutVisionConsoleFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonLookoutVisionConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 11 maggio 2021, 19:37 UTC
- Ora modificata: 11 maggio 2021, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketFirstUseSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDatasetLabelingToolsAccess",
      "Effect" : "Allow",
      "Action" : [
        "groundtruthlabeling:RunGenerateManifestByCrawlingJob",
        "groundtruthlabeling:AssociatePatchToManifestJob",
        "groundtruthlabeling:DescribeConsoleJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleTagSelectorAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleKmsKeySelectorAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLookoutVisionConsoleReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Lookout for Vision e accesso mirato al servizio richiesto e alle dipendenze della console.

`AmazonLookoutVisionConsoleReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonLookoutVisionConsoleReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 11 maggio 2021, 19:32 UTC
- Ora modificata: 09 dicembre 2021, 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeTrialDetection",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListTrialDetections",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLookoutVisionFullAccess

Descrizione: fornisce accesso completo ad Amazon Lookout for Vision e accesso mirato alle dipendenze richieste.

`AmazonLookoutVisionFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonLookoutVisionFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2021, 19:24 UTC
- Ora modificata: 11 maggio 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonLookoutVisionReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Lookout for Vision e accesso mirato alle dipendenze richieste.

`AmazonLookoutVisionReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonLookoutVisionReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2021, 19:11 UTC
- Ora modificata: 09 dicembre 2021, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMachineLearningBatchPredictionsAccess

Descrizione: concede agli utenti l'autorizzazione a richiedere previsioni in batch su Amazon Machine Learning.

`AmazonMachineLearningBatchPredictionsAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMachineLearningBatchPredictionsAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:12 UTC
- Ora modificata: 9 aprile 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMachineLearningCreateOnlyAccess

Descrizione: fornisce accesso diretto a risorse Amazon Machine Learning non predittive.

`AmazonMachineLearningCreateOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMachineLearningCreateOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:18 UTC
- Ora modificata: 29 giugno 2016, 20:55 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMachineLearningFullAccess

Descrizione: fornisce l'accesso completo alle risorse di Amazon Machine Learning.

`AmazonMachineLearningFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMachineLearningFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:25 UTC
- Ora modificata: 9 aprile 2015, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

Descrizione: concede agli utenti l'autorizzazione a creare ed eliminare l'endpoint in tempo reale per i modelli di Amazon Machine Learning.

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMachineLearningManageRealTimeEndpointOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:32 UTC
- Ora modificata: 9 aprile 2015, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateRealtimeEndpoint",
        "machinelearning:DeleteRealtimeEndpoint"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMachineLearningReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle risorse di Amazon Machine Learning.

`AmazonMachineLearningReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMachineLearningReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:40 UTC
- Ora modificata: 9 aprile 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMachineLearningRealTimePredictionOnlyAccess

Descrizione: concede agli utenti l'autorizzazione a richiedere previsioni in tempo reale di Amazon Machine Learning.

`AmazonMachineLearningRealTimePredictionOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMachineLearningRealTimePredictionOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 aprile 2015, 17:44 UTC
- Ora modificata: 9 aprile 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Predict"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMachineLearningRoleforRedshiftDataSourceV3

Descrizione: consente al Machine Learning di configurare e utilizzare i cluster Redshift e le location di staging S3 per Redshift Data Source.

`AmazonMachineLearningRoleforRedshiftDataSourceV3`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonMachineLearningRoleforRedshiftDataSourceV3` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 giugno 2020, 18:00 UTC
- Ora modificata: 24 giugno 2020, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupIngress",
        "redshift:AuthorizeClusterSecurityGroupIngress",
        "redshift:CreateClusterSecurityGroup",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:ModifyCluster",
        "redshift:RevokeClusterSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::amazon-machine-learning*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMacieFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Macie.

`AmazonMacieFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMacieFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 agosto 2017, 14:54 UTC
- Ora modificata: 01 luglio 2022, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "pricing:GetProducts",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMacieHandshakeRole

Descrizione: concede l'autorizzazione a creare il ruolo collegato al servizio di Amazon Macie.

`AmazonMacieHandshakeRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonMacieHandshakeRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 28 giugno 2018, 15:46 UTC
- Ora modificata: 28 giugno 2018, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMacieReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon Macie.

`AmazonMacieReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMacieReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 15 giugno 2023, 21:50 UTC
- Ora modificata: 15 giugno 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMacieServiceRole

Descrizione: concede a Macie l'accesso in sola lettura alle dipendenze delle risorse del tuo account per consentire l'analisi dei dati.

`AmazonMacieServiceRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonMacieServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 14:53 UTC
- Ora modificata: 14 agosto 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMacieServiceRolePolicy

Descrizione: ruolo collegato al servizio per Amazon Macie

`AmazonMacieServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 giugno 2018, 22:17 UTC
- Ora modificata: 19 maggio 2022, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonManagedBlockchainConsoleFullAccess

Descrizione: Fornisce l'accesso completo ad Amazon Managed Blockchain tramite Console di gestione AWS

`AmazonManagedBlockchainConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonManagedBlockchainConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 aprile 2019, 21:23 UTC
- Ora modificata: 29 aprile 2019, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonManagedBlockchainFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Managed Blockchain.

`AmazonManagedBlockchainFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonManagedBlockchainFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 aprile 2019, 21:39 UTC
- Ora modificata: 29 aprile 2019, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonManagedBlockchainReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Managed Blockchain.

`AmazonManagedBlockchainReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonManagedBlockchainReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 aprile 2019, 18:17 UTC
- Ora modificata: 30 aprile 2019, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:Get*",
        "managedblockchain:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonManagedBlockchainServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Amazon Managed Blockchain

`AmazonManagedBlockchainServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 gennaio 2020, 19:51 UTC

- Ora modificata: 17 gennaio 2020, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*:log-stream:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMCSFullAccess

Descrizione: Fornisci l'accesso completo al servizio Amazon Managed Apache Cassandra

`AmazonMCSFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMCSFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 13:45 UTC
- Ora modificata: 17 aprile 2020, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
```

```
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMCSReadOnlyAccess

Descrizione: Fornisci accesso in sola lettura al servizio Amazon Managed Apache Cassandra

`AmazonMCSReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMCSReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 13:46 UTC
- Ora modificata: 17 aprile 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMechanicalTurkFullAccess

Descrizione: fornisce l'accesso completo a tutto APIs in Amazon Mechanical Turk.

`AmazonMechanicalTurkFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMechanicalTurkFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2015, 19:08 UTC
- Ora modificata: 11 dicembre 2015, 19:08 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mechanicalturk:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMechanicalTurkReadOnly

Descrizione: fornisce l'accesso alla sola lettura APIs in Amazon Mechanical Turk.

`AmazonMechanicalTurkReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMechanicalTurkReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2015, 19:08 UTC
- Ora modificata: 25 settembre 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mechanicalturk:Get*",
        "mechanicalturk:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMemoryDBFullAccess

Descrizione: fornisce l'accesso completo ad Amazon MemoryDB tramite. Console di gestione AWS

`AmazonMemoryDBFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMemoryDBFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 08 ottobre 2021, 19:24 UTC
- Ora modificata: 08 ottobre 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : "memorydb:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/memorydb.amazonaws.com/
AWSServiceRoleForMemoryDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "memorydb.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMemoryDBReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon MemoryDB tramite. Console di gestione AWS

`AmazonMemoryDBReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMemoryDBReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 08 ottobre 2021, 19:27 UTC

- Ora modificata: 08 ottobre 2021, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "memorydb:Describe*",
        "memorydb:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMobileAnalyticsFinancialReportAccess

Descrizione: fornisce l'accesso in sola lettura a tutti i report, inclusi i dati finanziari per tutte le risorse dell'applicazione.

`AmazonMobileAnalyticsFinancialReportAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMobileAnalyticsFinancialReportAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mobileanalytics:GetReports",
        "mobileanalytics:GetFinancialReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMobileAnalyticsFullAccess

Descrizione: fornisce l'accesso completo a tutte le risorse dell'applicazione.

`AmazonMobileAnalyticsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMobileAnalyticsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : "mobileanalytics:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMobileAnalyticsNon-financialReportAccess

Descrizione: fornisce l'accesso in sola lettura ai report non finanziari per tutte le risorse dell'applicazione.

`AmazonMobileAnalyticsNon-financialReportAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMobileAnalyticsNon-financialReportAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:GetReports",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMobileAnalyticsWriteOnlyAccess

Descrizione: fornisce l'accesso in sola scrittura ai dati degli eventi put per tutte le risorse dell'applicazione. (Consigliato per l'integrazione con SDK)

`AmazonMobileAnalyticsWriteOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMobileAnalyticsWriteOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:PutEvents",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMonitronFullAccess

Descrizione: Fornisce l'accesso completo per gestire Amazon Monitron

`AmazonMonitronFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMonitronFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 dicembre 2020, 22:40 UTC
- Ora modificata: 08 giugno 2022, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitron.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "monitron:*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "monitron.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "AWSSSOPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/monitron/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMQApiFullAccess

Descrizione: fornisce l'accesso completo ad AmazonMQ tramite la nostra API/SDK.

`AmazonMQApiFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonMQApiFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 dicembre 2018, 20:31 UTC
- Ora modificata: 04 novembre 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMQApiReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad AmazonMQ tramite la nostra API/SDK.

`AmazonMQApiReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonMQApiReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 dicembre 2018, 20:31 UTC
- Ora modificata: 18 dicembre 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMQFullAccess

Descrizione: fornisce l'accesso completo ad AmazonMQ tramite. Console di gestione AWS

`AmazonMQFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMQFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2017, 15:28 UTC
- Ora modificata: 04 novembre 2020, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "cloudformation:CreateStack",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMQReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad AmazonMQ tramite. Console di gestione AWS

`AmazonMQReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMQReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2017, 15:30 UTC
- Ora modificata: 28 novembre 2017, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMQServiceRolePolicy

Descrizione: Policy Service Linked Role per AWS Amazon MQ

`AmazonMQServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 4 novembre 2020, 16:07 UTC
- Ora modificata: 04 novembre 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMSKConnectReadOnlyAccess

Descrizione: Fornisci accesso in sola lettura ad Amazon MSK Connect

`AmazonMSKConnectReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMSKConnectReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 20 settembre 2021, 10:18 UTC
- Ora modificata: 18 ottobre 2021, 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeConnector"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:connector/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeCustomPlugin"
      ],
      "Resource" : [
```

```
        "arn:aws:kafkaconnect:*:*:custom-plugin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeWorkerConfiguration"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:worker-configuration/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMSKFullAccess

Descrizione: Fornisci l'accesso completo ad Amazon MSK e ad altre autorizzazioni richieste per le sue dipendenze.

`AmazonMSKFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonMSKFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 gennaio 2019, 22:07 UTC
- Ora modificata: 18 ottobre 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:*",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "S3:GetBucketPolicy",
        "firehose:TagDeliveryStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
```

```
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "aws:RequestTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
```

```
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/
AWSServiceRoleForKafka*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMSKReadOnlyAccess

Descrizione: Fornisci l'accesso in sola lettura ad Amazon MSK

`AmazonMSKReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonMSKReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 gennaio 2019, 22:28 UTC
- Ora modificata: 14 gennaio 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "kafka:Describe*",
        "kafka:List*",
        "kafka:Get*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMWAAServerlessServiceRolePolicy

Descrizione: Fornisce l'accesso ad Amazon Airflow Serverless Service per gestire le reti per i flussi di lavoro e accedere ad altri AWS servizi per tuo conto

`AmazonMWAAServerlessServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 novembre 2025, 20:34 UTC

- Ora modificata: 15 novembre 2025, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServerlessServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonMWAAServiceRolePolicy

Descrizione: il ruolo collegato al servizio utilizzato da Amazon Managed Workflows per Apache Airflow.

`AmazonMWAAServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 24 novembre 2020, 14:13 UTC
- Ora modificata: 17 novembre 2022, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
```

```
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:airflow-*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonMWAAManaged" : false
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/MWAA"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonNimbleStudio-LaunchProfileWorker

Descrizione: questa politica consente l'accesso alle risorse necessarie ai lavoratori di Nimble Studio Launch Profile. Allega questa policy alle istanze EC2 create da Nimble Studio Builder.

`AmazonNimbleStudio-LaunchProfileWorker`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonNimbleStudio-LaunchProfileWorker` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 aprile 2021, 04:47 UTC
- Ora modificata: 28 aprile 2021, 04:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      },
      "Sid" : "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonNimbleStudio-StudioAdmin

Descrizione: questa politica consente l'accesso alle risorse di Amazon Nimble Studio associate all'amministratore dello studio e alle risorse di studio correlate in altri servizi. Allega questa policy al ruolo di amministratore associato al tuo studio.

`AmazonNimbleStudio-StudioAdmin`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonNimbleStudio-StudioAdmin` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 aprile 2021, 04:47 UTC
- Ora modificata: 22 settembre 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Sid" : "StudioAdminFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
```

```
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonNimbleStudio-StudioUser

Descrizione: questa politica consente l'accesso alle risorse di Amazon Nimble Studio associate all'utente dello studio e alle risorse di studio correlate in altri servizi. Allega questa politica al ruolo Utente associato al tuo studio.

`AmazonNimbleStudio-StudioUser`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonNimbleStudio-StudioUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 aprile 2021, 04:48 UTC
- Ora modificata: 22 settembre 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListLaunchProfiles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:requesterPrincipalId" : "${nimble:principalId}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "nimble:ownedBy" : "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonODBFullAccess

Descrizione: fornisce l'accesso completo alle risorse in Oracle Database@AWS

`AmazonODBFullAccess`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonODBFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 luglio 2026, 22:57 UTC
- Ora modificata: 23 luglio 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonODBFullAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructure",
        "odb:UpdateCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:DeleteCloudExadataInfrastructure",
        "odb:ListCloudExadataInfrastructures",
        "odb:CreateCloudVmCluster",
        "odb:GetCloudVmCluster",
        "odb:DeleteCloudVmCluster",
        "odb:ListCloudVmClusters",
        "odb:CreateCloudAutonomousVmCluster",
        "odb:GetCloudAutonomousVmCluster",
        "odb:DeleteCloudAutonomousVmCluster",
        "odb:ListCloudAutonomousVmClusters",
        "odb:CreateAutonomousDatabase",
        "odb:GetAutonomousDatabase",
        "odb:UpdateAutonomousDatabase",
        "odb:DeleteAutonomousDatabase",
        "odb:ListAutonomousDatabases",
        "odb:ListAutonomousDatabaseClones",
        "odb:ListAutonomousDatabasePeers",
        "odb:StartAutonomousDatabase",
        "odb:StopAutonomousDatabase",
        "odb:RebootAutonomousDatabase",
        "odb:ShrinkAutonomousDatabase",
        "odb:SwitchoverAutonomousDatabase",
        "odb:FailoverAutonomousDatabase",
        "odb:RestoreAutonomousDatabase",
```

```
        "odb:CreateAutonomousDatabaseWallet",
        "odb:GetAutonomousDatabaseWalletDetails",
        "odb:CreateAutonomousDatabaseBackup",
        "odb:GetAutonomousDatabaseBackup",
        "odb:UpdateAutonomousDatabaseBackup",
        "odb:DeleteAutonomousDatabaseBackup",
        "odb:ListAutonomousDatabaseBackups",
        "odb:CreateDbNode",
        "odb:GetDbNode",
        "odb:RebootDbNode",
        "odb:StartDbNode",
        "odb:StopDbNode",
        "odb:DeleteDbNode",
        "odb:ListDbNodes",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:CreateOdbNetwork",
        "odb:GetOdbNetwork",
        "odb:UpdateOdbNetwork",
        "odb:DeleteOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:CreateOdbPeeringConnection",
        "odb:GetOdbPeeringConnection",
        "odb:UpdateOdbPeeringConnection",
        "odb:DeleteOdbPeeringConnection",
        "odb:ListOdbPeeringConnections",
        "odb:ListAutonomousVirtualMachines",
        "odb:ListDbSystemShapes",
        "odb:ListGiVersions",
        "odb:ListSystemVersions",
        "odb:ListAutonomousDatabaseVersions",
        "odb:ListAutonomousDatabaseCharacterSets",
        "odb:PutResourcePolicy",
        "odb:GetResourcePolicy",
        "odb:DeleteResourcePolicy",
        "odb:CreateOutboundIntegration",
        "odb:TagResource",
        "odb:UntagResource",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOdbNetworkPeeringActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateOdbNetworkPeering",
        "ec2:ModifyOdbNetworkPeering",
        "ec2:DeleteOdbNetworkPeering"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "odb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "odb.amazonaws.com",
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonODBServiceRolePolicy

Descrizione: consente a Oracle Database@AWS di gestire AWS le risorse per tuo conto.

`AmazonODBServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 13 novembre 2024, 18:21 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonODBServiceRolePolicy`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ODB"
          ]
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NM",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EB1",
      "Effect" : "Allow",
      "Action" : [
        "events:ActivateEventSource",
        "events:DescribeEventSource"
      ],
      "Resource" : "arn:aws:events:*:*:event-source/aws.partner/odb*"
    },
```

```
    {
      "Sid" : "EB2",
      "Effect" : "Allow",
      "Action" : [
        "events:CreateEventBus",
        "events:DescribeEventBus"
      ],
      "Resource" : "arn:aws:events:*:*:event-bus/aws.partner/odb*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOmicsFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Omics e ad altri requisiti richiesti. Servizi AWS Questa politica consente all'utente di visualizzare e accettare gli inviti alla condivisione RAM per accedere a risorse esterne a quelle dell'utente. Account AWS

`AmazonOmicsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOmicsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 febbraio 2023, 00:59 UTC
- Ora modificata: 24 febbraio 2023, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "omics.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "omics.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOmicsReadOnlyAccess

Descrizione: Fornisci l'accesso in sola lettura ad Amazon Omics

`AmazonOmicsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOmicsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2022, 04:17 UTC
- Ora modificata: 29 novembre 2022, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:Get*",
        "omics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOneEnterpriseFullAccess

Descrizione: questa politica concede autorizzazioni amministrative che consentono l'accesso a tutte le risorse e le operazioni di Amazon One Enterprise.

`AmazonOneEnterpriseFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOneEnterpriseFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2023, 04:58 UTC
- Ora modificata: 28 novembre 2023, 04:58 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOneEnterpriseInstallerAccess

Descrizione: questa politica concede autorizzazioni di lettura e scrittura limitate che consentono l'installazione e l'attivazione del dispositivo.

`AmazonOneEnterpriseInstallerAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOneEnterpriseInstallerAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2023, 05:00 UTC
- Ora modificata: 28 novembre 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOneEnterpriseReadOnlyAccess

Descrizione: questa politica concede autorizzazioni di sola lettura a tutte le risorse e le operazioni di Amazon One Enterprise.

`AmazonOneEnterpriseReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOneEnterpriseReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2023, 04:59 UTC
- Ora modificata: 28 novembre 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:Get*",
        "one:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOpenSearchDashboardsServiceRolePolicy

Descrizione: Fornisce l'accesso ad Amazon OpenSearch Dashboards Service per accedere ad altri AWS servizi, ad esempio per tuo CloudWatch conto

`AmazonOpenSearchDashboardsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 22 dicembre 2023, 19:38 UTC
- Ora modificata: 22 dicembre 2023, 19:38 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDashboardsServiceRoleAllowedActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSD"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOpenSearchDirectQueryGlueCreateAccess

Descrizione: consente a OpenSearch DirectQuery Service di accedere a AWS Glue APIs per creare risorse per tuo conto.

`AmazonOpenSearchDirectQueryGlueCreateAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOpenSearchDirectQueryGlueCreateAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 maggio 2024, 12:24 UTC
- Ora modificata: 06 maggio 2024, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOpenSearchIngestionFullAccess

Descrizione: consente ad Amazon OpenSearch Ingestion di accedere ad altri AWS servizi per tuo conto.

`AmazonOpenSearchIngestionFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOpenSearchIngestionFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 aprile 2023, 18:11 UTC
- Ora modificata: 26 aprile 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:CreatePipeline",
        "osis:UpdatePipeline",
        "osis:DeletePipeline",
        "osis:StartPipeline",
        "osis:StopPipeline",
        "osis:ListPipelines",
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:ValidatePipeline",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:TagResource",
        "osis:UntagResource",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/osis.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchIngestionService",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "osis.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOpenSearchIngestionReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon OpenSearch Ingestion Service

`AmazonOpenSearchIngestionReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOpenSearchIngestionReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 aprile 2023, 18:09 UTC
- Ora modificata: 26 aprile 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
```

```
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOpenSearchIngestionServiceRolePolicy

Descrizione: consente ad Amazon OpenSearch Ingestion Service di accedere ad altri AWS servizi per tuo conto.

`AmazonOpenSearchIngestionServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 novembre 2022, 16:49 UTC
- Ora modificata: 28 agosto 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OSISManaged" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOpenSearchServerlessServiceRolePolicy

Descrizione: consenti ad Amazon OpenSearch Serverless di accedere ad altri AWS servizi, ad esempio per tuo CloudWatch APIs conto.

`AmazonOpenSearchServerlessServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 24 novembre 2022, 19:50 UTC
- Ora modificata: 25 luglio 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAOSSCloudwatchMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSS"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOpenSearchServiceCognitoAccess

Descrizione: fornisce l'accesso al servizio di configurazione Amazon Cognito.

`AmazonOpenSearchServiceCognitoAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOpenSearchServiceCognitoAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 settembre 2021, 06:31 UTC
- Ora modificata: 20 dicembre 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : [
        "arn:aws:cognito-identity:*:*:identitypool/*",
        "arn:aws:cognito-idp:*:*:userpool/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cognito-identity:SetIdentityPoolRoles",
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOpenSearchServiceFullAccess

Descrizione: fornisce l'accesso completo al servizio di configurazione OpenSearch di Amazon Service.

`AmazonOpenSearchServiceFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOpenSearchServiceFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 08 settembre 2021, 05:33 UTC
- Ora modificata: 08 settembre 2021, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOpenSearchServiceReadOnlyAccess

Descrizione: fornisce accesso in sola lettura al servizio di configurazione di Amazon OpenSearch Service.

`AmazonOpenSearchServiceReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonOpenSearchServiceReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 08 settembre 2021, 05:38 UTC

- Ora modificata: 08 settembre 2021, 05:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:Describe*",
        "es:List*",
        "es:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonOpenSearchServiceRolePolicy

Descrizione: consenti ad Amazon OpenSearch Service di accedere ad altri AWS servizi come EC2 Networking per tuo APIs conto.

`AmazonOpenSearchServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 agosto 2021, 09:27 UTC
- Ora modificata: 27 marzo 2025, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973144",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973165",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973154",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973164",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973174",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973184",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973195",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973196",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973197",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ES",
            "AWS/OpenSearch"
          ]
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sso:PutApplicationAccessScope",
      "Resource" : "arn:aws:sso::*:application/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonPersonalizeFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Personalize tramite l'SDK Console di gestione AWS and. Fornisce inoltre un accesso selezionato ai servizi correlati (ad esempio, S3,). CloudWatch

`AmazonPersonalizeFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonPersonalizeFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 4 dicembre 2018, 22:24 UTC
- Ora modificata: 30 maggio 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "personalize:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::*Personalize*",
        "arn:aws:s3:::*personalize*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "personalize.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonPollyFullAccess

Descrizione: garantisce l'accesso completo al servizio e alle risorse Amazon Polly.

`AmazonPollyFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonPollyFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2016, 18:59 UTC

- Ora modificata: 30 novembre 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonPollyReadOnlyAccess

Descrizione: concede l'accesso in sola lettura alle risorse di Amazon Polly.

`AmazonPollyReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonPollyReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2016, 18:59 UTC
- Ora modificata: 01 aprile 2026, 08:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech",
        "polly:StartSpeechSynthesisStream"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonPrometheusConsoleFullAccess

Descrizione: concede l'accesso completo alle risorse AWS gestite di Prometheus nella console AWS

`AmazonPrometheusConsoleFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonPrometheusConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 18:11 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
        "aps:DeleteWorkspace",
        "aps:ListWorkspaces",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:CreateAlertManagerDefinition",
        "aps:CreateRuleGroupsNamespace",
        "aps:DeleteAlertManagerDefinition",
        "aps:DeleteRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:PutAlertManagerDefinition",
        "aps:PutRuleGroupsNamespace",
        "aps:TagResource",
        "aps:UntagResource",
        "aps:CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps:DeleteLoggingConfiguration",
        "aps:DescribeLoggingConfiguration",
        "aps:UpdateWorkspaceConfiguration",
        "aps:DescribeWorkspaceConfiguration",
        "aps:CreateQueryLoggingConfiguration",
        "aps:UpdateQueryLoggingConfiguration",
        "aps:DeleteQueryLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonPrometheusFullAccess

Descrizione: Garantisce l'accesso completo alle risorse AWS gestite di Prometheus

`AmazonPrometheusFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonPrometheusFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 18:10 UTC
- Ora modificata: 26 novembre 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scraper.aps.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonPrometheusQueryAccess

Descrizione: concede l'accesso per eseguire query sulle risorse gestite di AWS Prometheus

`AmazonPrometheusQueryAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonPrometheusQueryAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 dicembre 2020, 01:02 UTC
- Ora modificata: 19 dicembre 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonPrometheusRemoteWriteAccess

Descrizione: concede l'accesso in sola scrittura alle aree di lavoro AWS gestite di Prometheus

`AmazonPrometheusRemoteWriteAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonPrometheusRemoteWriteAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 dicembre 2020, 01:04 UTC
- Ora modificata: 19 dicembre 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:RemoteWrite"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonPrometheusScraperServiceRolePolicy

Descrizione: fornisce l'accesso alle AWS risorse gestite o utilizzate da Amazon Managed Service per Prometheus Collector

`AmazonPrometheusScraperServiceRolePolicy`è una policy gestita. AWS

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 26 novembre 2023, 14:19 UTC
- Ora modificata: 17 luglio 2026, 08:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

Versione della politica

Versione della politica: v3 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScraper"
          ]
        }
      }
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "ENIUpdating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AMPAgentlessScraper" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "EKSAccess",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DeleteEKSAccessEntry",
      "Effect" : "Allow",
      "Action" : "eks:DeleteAccessEntry",
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/
scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
        }
      }
    },
    {
      "Sid" : "APSWriting",
      "Effect" : "Allow",
      "Action" : "aps:RemoteWrite",
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetricsWriting",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "arn:aws:cloudwatch:*:*:dataset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonQDeveloperAccess

Descrizione: Fornisce l'accesso agli sviluppatori per abilitare le interazioni con Amazon Q

`AmazonQDeveloperAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonQDeveloperAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 luglio 2024, 08:35 UTC
- Ora modificata: 20 maggio 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQDeveloperAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AllowAmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:StartTroubleshootingResolutionExplanation",
        "q:GetTroubleshootingResults",
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetaData",
        "q:GenerateCodeFromCommands",
        "q:UsePlugin"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "AllowQArtifactsAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateArtifact",
```

```
        "q:GetArtifact",
        "q:GetArtifactActionResult",
        "q:PerformArtifactAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonQFullAccess

Descrizione: Fornisce l'accesso completo per abilitare le interazioni con Amazon Q

`AmazonQFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonQFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2023, 16:00 UTC
- Ora modificata: 20 maggio 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetadata",
        "q:CreateAssignment",
        "q:DeleteAssignment",
        "q:GenerateCodeFromCommands",
        "q:CreatePlugin",
        "q:UpdatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin",
        "q:UsePlugin",
        "q:ListPlugins",
        "q:ListPluginProviders",
        "q:ListTagsForResource",
        "q:UntagResource",
        "q:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowQArtifactsAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "q:CreateArtifact",
        "q:GetArtifact",
        "q:GetArtifactActionResult",
        "q:PerformArtifactAction"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "AllowPassRoleToAmazonQ",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "q.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonQLDBConsoleFullAccess

Descrizione: fornisce l'accesso completo ad Amazon QLDB tramite. Console di gestione AWS

`AmazonQLDBConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonQLDBConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 settembre 2019, 18:24 UTC
- Ora modificata: 04 novembre 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:ExecuteStatement",
        "qldb:ShowCatalog",
        "qldb:InsertSampleData",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonQLDBFullAccess

Descrizione: fornisce l'accesso completo ad Amazon QLDB tramite l'API del servizio.

`AmazonQLDBFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonQLDBFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 settembre 2019, 18:23 UTC
- Ora modificata: 04 novembre 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:GetBlock",
```

```
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonQLDBReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon QLDB.

`AmazonQLDBReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonQLDBReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 settembre 2019, 18:19 UTC
- Ora modificata: 02 luglio 2021, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
```

```
        "qldb:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSBetaServiceRolePolicy

Descrizione: consente ad Amazon RDS di gestire AWS le risorse per tuo conto.

`AmazonRDSBetaServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 2 maggio 2018, 19:41 UTC
- Ora modificata: 07 agosto 2024, 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSCustomInstanceProfileRolePolicy

Descrizione: consente ad Amazon RDS Custom di eseguire varie azioni di automazione e attività di gestione del database tramite un profilo di istanza EC2.

`AmazonRDSCustomInstanceProfileRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRDSCustomInstanceProfileRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 febbraio 2024, 17:42 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssmAgentPermission4",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenControlChannel"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ssmAgentPermission5",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "createEc2SnapshotPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createTagForEc2SnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "CreateSnapshots"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "rdsCustomS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "rdsCustomS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "readSecretsFromCpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
```

```
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createSecretsOnDpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "publishCwMetricsPermission",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "rdscustom/rds-custom-sqlserver-agent",
            "RDSCustomForOracle/Agent"
          ]
        }
      }
    },
    {
      "Sid" : "putEventsToEventBusPermission",
```

```
      "Effect" : "Allow",
      "Action" : "events:PutEvents",
      "Resource" : "arn:aws:events:*:*:event-bus/default"
    },
    {
      "Sid" : "cwlUploadPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutRetentionPolicy",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:rds-custom-instance-*"
    },
    {
      "Sid" : "sendMessageToSqsQueuePermission",
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-sqlserver"
        }
      }
    },
    {
      "Sid" : "managePrivateIpOnEniPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithSecret",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" : [
            "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
            "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithS3",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-rds-custom-
*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSCustomPreviewServiceRolePolicy

Descrizione: politica del ruolo del servizio Amazon RDS Custom Preview

`AmazonRDSCustomPreviewServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 8 ottobre 2021, 21:44 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
```

```
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
```

```
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
```

```
        ]
      }
    }
  },
  {
    "Sid" : "eb3",
    "Effect" : "Allow",
    "Action" : [
      "events:PutRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "events:ManagedBy" : [
          "custom.rds-preview.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "eb4",
    "Effect" : "Allow",
    "Action" : [
      "events:PutTargets",
      "events:EnableRule",
      "events:DeleteRule",
      "events:RemoveTargets",
      "events:DisableRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "events:ManagedBy" : [
          "custom.rds-preview.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "eb5",
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:ListTargetsByRule"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RestoreSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSCustomServiceRolePolicy

Descrizione: consente ad Amazon RDS Custom di gestire AWS le risorse per tuo conto.

`AmazonRDSCustomServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 8 ottobre 2021, 21:39 UTC

- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Versione della politica

Versione della politica: v19 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "rdscrc",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
```

```
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "eccModifyInstanceAttribute1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ],
          "ec2:Attribute" : "InstanceType"
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
```

```
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshot",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress",
            "CopyImage"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
```

```
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccAmi1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ]
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AWSRDSCustom*",
        "arn:aws:iam::*:role/service-role/AWSRDSCustom*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
```

```
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RestoreSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-sqlserver",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSDataFullAccess

Descrizione: consente l'accesso completo all'utilizzo dei dati RDS APIs, all'archivio segreto APIs per le credenziali del database RDS e APIs alla gestione delle query della console DB per eseguire istruzioni SQL sui cluster Aurora Serverless in. Account AWS

`AmazonRDSDataFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonRDSDataFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2018, 21:29 UTC
- Ora modificata: 20 novembre 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerDbCredentialsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
    },
    {
      "Sid" : "RDSDataServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory",
        "rds-data:ExecuteSql",
        "rds-data:ExecuteStatement",
        "rds-data:BatchExecuteStatement",
        "rds-data:BeginTransaction",
        "rds-data:CommitTransaction",
        "rds-data:RollbackTransaction",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
```

```
        "secretsmanager:GetRandomPassword",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSDirectoryServiceAccess

Descrizione: consente a RDS di accedere a Directory Service Managed AD per conto del cliente per le istanze DB di SQL Server aggiunte al dominio.

`AmazonRDSDirectoryServiceAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonRDSDirectoryServiceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 febbraio 2016, 02:02 UTC
- Ora modificata: 15 maggio 2019, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSEnhancedMonitoringRole

Descrizione: fornisce l'accesso a Cloudwatch for RDS Enhanced Monitoring

`AmazonRDSEnhancedMonitoringRole`è una policy gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonRDSEnhancedMonitoringRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 novembre 2015, 19:58 UTC
- Ora modificata: 11 novembre 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*:log-stream:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSFullAccess

Descrizione: fornisce l'accesso completo ad Amazon RDS tramite. Console di gestione AWS

`AmazonRDSFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRDSFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 17 agosto 2023, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:GetCoipPoolUsage",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "outposts:GetOutpostInstanceTypes",
        "devops-guru:GetResourceCollection"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "pi:*",
      "Resource" : [
        "arn:aws:pi:*:*:metrics/rds/*",
        "arn:aws:pi:*:*:perf-reports/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "rds.amazonaws.com",
            "rds.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSPerformanceInsightsFullAccess

Descrizione: fornisce l'accesso completo a RDS Performance Insights tramite Console di gestione AWS

`AmazonRDSPerformanceInsightsFullAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRDSPerformanceInsightsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 agosto 2023, 23:41 UTC
- Ora modificata: 23 luglio 2026, 00:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Versione della politica

Versione della politica: v6 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:CreatePerformanceAnalysisReport",
        "pi:GetPerformanceAnalysisReport",
        "pi:ListPerformanceAnalysisReportRecommendations",
        "pi:ListPerformanceAnalysisReports",
        "pi:DeletePerformanceAnalysisReport"
      ],
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:TagResource",
        "pi:UntagResource",
        "pi:ListTagsForResource"
      ],
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    },
    {
      "Sid" : "AmazonRDSDescribeInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:ListTagsForResource",
```

```
        "rds:DescribeDBShardGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:shard-group:*"
      ]
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSPerformanceInsightsReadOnly

Descrizione: Read-Only politica per RDS Performance Insights

`AmazonRDSPerformanceInsightsReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRDSPerformanceInsightsReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 05 aprile 2022, 00:02 UTC
- Ora modificata: 22 luglio 2026, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Versione della politica

Versione della politica: v7 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBShardGroups",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBShardGroups",
      "Resource" : "arn:aws:rds:*:*:shard-group:*"
    },
    {
      "Sid" : "AmazonRDSListTagsForResource",
```

```
      "Effect" : "Allow",
      "Action" : "rds:ListTagsForResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:shard-group:*",
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
      "Effect" : "Allow",
      "Action" : "pi:DescribeDimensionKeys",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
      "Effect" : "Allow",
      "Action" : "pi:GetDimensionKeyDetails",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetadata",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceDimensions",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
```

```
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
      "Effect" : "Allow",
      "Action" : "pi:GetPerformanceAnalysisReport",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" :
 "AmazonRDSPerformanceInsightsListPerformanceAnalysisReportRecommendations",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReportRecommendations",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReports",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
      "Effect" : "Allow",
      "Action" : "pi:ListTagsForResource",
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSPreviewServiceRolePolicy

Descrizione: Politica sul ruolo del servizio Amazon RDS Preview

`AmazonRDSPreviewServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 31 maggio 2018, 18:02 UTC
- Ora modificata: 07 agosto 2024, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
```

```
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Preview",
            "AWS/Neptune-Preview",
            "AWS/RDS-Preview",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon RDS tramite. Console di gestione AWS

`AmazonRDSReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRDSReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 14 aprile 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "devops-guru:GetResourceCollection"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRDSServiceRolePolicy

Descrizione: consente ad Amazon RDS di gestire AWS le risorse per tuo conto.

`AmazonRDSServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 8 gennaio 2018, 18:17 UTC
- Ora modificata: 01 luglio 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossRegionCommunication",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ]
```

```
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "Kinesis",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream",
        "kinesis:SplitShard",
        "kinesis:MergeShards",
        "kinesis:DeleteStream",
        "kinesis:UpdateShardCount"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
      ]
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
```

```
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    },
    {
      "Sid" : "SecretsManagerTags",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
```

```
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftAllCommandsFullAccess

Descrizione: questa policy include le autorizzazioni per eseguire comandi SQL per copiare, caricare, scaricare, interrogare e analizzare i dati su Amazon Redshift. La policy concede inoltre le autorizzazioni per eseguire istruzioni selezionate per servizi correlati, come Amazon S3, Amazon logs, CloudWatch SageMaker Amazon o Glue. AWS

`AmazonRedshiftAllCommandsFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonRedshiftAllCommandsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 04 novembre 2021, 00:48 UTC
- Ora modificata: 25 novembre 2021, 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "SageMaker",
            "/aws/sagemaker/Endpoints",
            "/aws/sagemaker/ProcessingJobs",
            "/aws/sagemaker/TrainingJobs",
            "/aws/sagemaker/TransformJobs"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3:::*redshift*",
        "arn:aws:s3:::*redshift*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/Redshift" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:DescribeTable",
```

```
        "dynamodb:Getitem"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*redshift*",
        "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListInstances"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "elasticmapreduce:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*redshift*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
```

```
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "redshift.amazonaws.com",
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "athena.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftDataFullAccess

Descrizione: questa policy fornisce l'accesso completo ai dati di Amazon Redshift. APIs Questa politica garantisce anche l'accesso mirato ad altri servizi richiesti.

`AmazonRedshiftDataFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRedshiftDataFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 settembre 2020, 19:23 UTC
- Ora modificata: 07 aprile 2023, 18:18 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "GetCredentialsForAPIUser",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "GetCredentialsWithFederatedIAMCredentials",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentialsWithIAM",
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*"
    },
    {
      "Sid" : "GetCredentialsForServerless",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetCredentials",
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "DenyCreateAPIUser",
      "Effect" : "Deny",
      "Action" : "redshift:CreateClusterUser",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "ServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift-data.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : "redshift-data.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftFederatedAuthorization

Descrizione: questa è una ease-of-use politica per l'esecuzione di query con Amazon Redshift Federated Authorization

`AmazonRedshiftFederatedAuthorization`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonRedshiftFederatedAuthorization` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 novembre 2025, 00:04 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFederatedAuthorization`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftFederatedAuthorization",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetUserDefinedFunctions",
        "glue:CreateDatabase",
        "glue:CreateTable",
        "glue:DeleteDatabase",
        "glue:DeleteTable",
        "glue:UpdateCatalog",
        "glue:UpdateDatabase",
        "glue:UpdateTable",
        "glue:RenameTable",
        "glue:FederateAuthorization"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:FederatedAuthorizationSource" : "Redshift"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftIdentityCenterSetContext",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Redshift tramite. Console di gestione AWS

`AmazonRedshiftFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRedshiftFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 07 luglio 2022, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DisableAlarmActions",
        "tag:GetResources",
        "tag:UntagResources",
        "tag:GetTagValues",
        "tag:GetTagKeys",
        "tag:TagResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftQueryEditor

Descrizione: fornisce l'accesso completo ad Amazon Redshift Query Editor e alle query salvate tramite. Console di gestione AWS

`AmazonRedshiftQueryEditor`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRedshiftQueryEditor` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 ottobre 2018, 22:50 UTC
- Ora modificata: 16 febbraio 2021, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials",
        "redshift:ListSchemas",
        "redshift:ListTables",
        "redshift:ListDatabases",
        "redshift:ExecuteQuery",
        "redshift:FetchResults",
        "redshift:CancelQuery",
        "redshift:DescribeClusters",
        "redshift:DescribeQuery",
        "redshift:DescribeTable",
        "redshift:ViewQueriesFromConsole",
        "redshift:DescribeSavedQueries",
        "redshift:CreateSavedQuery",
        "redshift:DeleteSavedQueries",
        "redshift:ModifySavedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIIAMSessionPermissionsRestriction",
      "Action" : [
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:ListStatements"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftQueryEditorV2FullAccess

Descrizione: concede l'accesso completo alle operazioni e alle risorse di Amazon Redshift Query Editor V2. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Ciò include le autorizzazioni per elencare i cluster Amazon Redshift, leggere chiavi e alias AWS in KMS e gestire i segreti di Query Editor V2 in Secrets Manager. AWS

`AmazonRedshiftQueryEditorV2FullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonRedshiftQueryEditorV2FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 settembre 2021, 14:06 UTC
- Ora modificata: 21 febbraio 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
```

```
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KeyManagementServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*"
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2Permissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:*",
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftQueryEditorV2NoSharing

Descrizione: consente di lavorare con Amazon Redshift Query Editor V2 senza condividere risorse. Il titolare autorizzato può solo leggere, aggiornare ed eliminare le proprie risorse, ma non può condividerle. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Ciò include le autorizzazioni per elencare i cluster Amazon Redshift e gestire i segreti di Query Editor V2 del principale in Secrets Manager. AWS

`AmazonRedshiftQueryEditorV2NoSharing`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonRedshiftQueryEditorV2NoSharing` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 settembre 2021, 14:18 UTC
- Ora modificata: 21 febbraio 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
```

```
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
```

```
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftQueryEditorV2ReadSharing

Descrizione: consente di lavorare con Amazon Redshift Query Editor V2 con una condivisione limitata delle risorse. Il titolare autorizzato può leggere, scrivere e condividere le proprie risorse. Il

responsabile autorizzato può leggere le risorse condivise con il suo team ma non può aggiornarle. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Ciò include le autorizzazioni per elencare i cluster Amazon Redshift e gestire i segreti di Query Editor V2 del principale in Secrets Manager. AWS

`AmazonRedshiftQueryEditorV2ReadSharing`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonRedshiftQueryEditorV2ReadSharing` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 settembre 2021, 14:22 UTC
- Ora modificata: 21 febbraio 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
```

```
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
```

```
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
```

```
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftQueryEditorV2ReadWriteSharing

Descrizione: consente di utilizzare Amazon Redshift Query Editor V2 con condivisione di risorse. Il titolare autorizzato può leggere, scrivere e condividere le proprie risorse. Il principale concesso può leggere e aggiornare le risorse condivise con il suo team. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Ciò include le autorizzazioni per elencare i cluster Amazon Redshift e gestire i segreti di Query Editor V2 del principale in Secrets Manager. AWS

`AmazonRedshiftQueryEditorV2ReadWriteSharing`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonRedshiftQueryEditorV2ReadWriteSharing` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 settembre 2021, 14:25 UTC
- Ora modificata: 21 febbraio 2024, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
```

```
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
```

```
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
```

```
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
```

```
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadWriteAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
```

```
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Redshift tramite. Console di gestione AWS

`AmazonRedshiftReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRedshiftReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 08 febbraio 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftReadOnlyAccess",
      "Action" : [
        "redshift:Describe*",
        "redshift:ListRecommendations",
        "redshift:ViewQueriesInConsole",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:List*",
        "cloudwatch:Get*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRedshiftServiceLinkedRolePolicy

Descrizione: consente ad Amazon Redshift di chiamare i AWS servizi per tuo conto

`AmazonRedshiftServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 settembre 2017, 19:19 UTC
- Ora modificata: 19 febbraio 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2VpcPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PublicAccessCreateEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "PublicAccessReleaseEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CreateSecurityGroupWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "SecurityGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:ModifySecurityGroupRules",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsOnResources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSecurityGroup",
            "CreateSubnet",
            "CreateInternetGateway",
            "CreateRouteTable",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "VPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Redshift-Serverless",
            "AWS/Redshift"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "SecretManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:RotateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:redshift!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "redshift",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerRandomPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IPV6Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ServiceQuotasToCheckCustomerLimits",
      "Effect" : "Allow",
      "Action" : [
```

```
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
        "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
      ]
    },
    {
      "Sid" : "DiscoverRedshiftCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Bool" : {
          "glue:EnabledForRedshiftAutoDiscovery" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeFormationGetMetadataAccessForFederatedCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Bool" : {
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "glue.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRekognitionCustomLabelsFullAccess

Descrizione: questa politica specifica le autorizzazioni Rekognition e s3 richieste dalla funzionalità Amazon Rekognition Custom Labels.

`AmazonRekognitionCustomLabelsFullAccess`AWS è una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRekognitionCustomLabelsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 gennaio 2020, 19:18 UTC
- Ora modificata: 16 agosto 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*custom-labels*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CreateProject",
        "rekognition:CreateProjectVersion",
        "rekognition:StartProjectVersion",
        "rekognition:StopProjectVersion",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DeleteProject",
        "rekognition:DeleteProjectVersion",
        "rekognition:TagResource",
        "rekognition:UntagResource",
        "rekognition:ListTagsForResource",
        "rekognition:CreateDataset",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:UpdateDatasetEntries",
        "rekognition:DistributeDatasetEntries",
        "rekognition:DeleteDataset",
        "rekognition:CopyProjectVersion",
```

```
        "rekognition:PutProjectPolicy",
        "rekognition:ListProjectPolicies",
        "rekognition:DeleteProjectPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRekognitionFullAccess

Descrizione: Accesso a tutte le Amazon Rekognition APIs

`AmazonRekognitionFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonRekognitionFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2016, 14:40 UTC
- Ora modificata: 30 novembre 2016, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRekognitionReadOnlyAccess

Descrizione: accesso a tutti i riconoscimenti Read APIs

`AmazonRekognitionReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonRekognitionReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 30 novembre 2016, 14:58 UTC
- Ora modificata: 08 novembre 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRekognitionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CompareFaces",
        "rekognition:DetectFaces",
        "rekognition:DetectLabels",
        "rekognition:ListCollections",
        "rekognition:ListFaces",
        "rekognition:SearchFaces",
        "rekognition:SearchFacesByImage",
        "rekognition:DetectText",
        "rekognition:GetCelebrityInfo",
        "rekognition:RecognizeCelebrities",
        "rekognition:DetectModerationLabels",
        "rekognition:GetLabelDetection",
        "rekognition:GetFaceDetection",
        "rekognition:GetContentModeration",
        "rekognition:GetPersonTracking",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetFaceSearch",
        "rekognition:GetTextDetection",
        "rekognition:GetSegmentDetection",
        "rekognition:DescribeStreamProcessor",
```

```
        "rekognition:ListStreamProcessors",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DetectProtectiveEquipment",
        "rekognition:ListTagsForResource",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:ListProjectPolicies",
        "rekognition:ListUsers",
        "rekognition:SearchUsers",
        "rekognition:SearchUsersByImage",
        "rekognition:GetMediaAnalysisJob",
        "rekognition:ListMediaAnalysisJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRekognitionServiceRole

Descrizione: consente a Rekognition di chiamare i servizi per AWS tuo conto.

`AmazonRekognitionServiceRole`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonRekognitionServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 29 novembre 2017, 16:52 UTC
- Ora modificata: 29 novembre 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetMedia"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53AutoNamingFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni di denominazione automatica della Route 53.

`AmazonRoute53AutoNamingFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53AutoNamingFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 gennaio 2018, 18:40 UTC
- Ora modificata: 18 gennaio 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53AutoNamingReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutte le azioni di denominazione automatica della Route 53.

`AmazonRoute53AutoNamingReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53AutoNamingReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 gennaio 2018, 03:02 UTC
- Ora modificata: 18 gennaio 2018, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53AutoNamingRegistrantAccess

Descrizione: fornisce l'accesso a livello di registrante alle azioni di denominazione automatica della Route 53.

`AmazonRoute53AutoNamingRegistrantAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53AutoNamingRegistrantAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 marzo 2018, 22:33 UTC
- Ora modificata: 12 marzo 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53DomainsFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni di Route53 Domains e Create Hosted Zone per consentire la creazione di Hosted Zone come parte delle registrazioni di domini.

`AmazonRoute53DomainsFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53DomainsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53DomainsReadOnlyAccess

Descrizione: fornisce l'accesso all'elenco e alle azioni dei domini Route53.

`AmazonRoute53DomainsReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53DomainsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53FullAccess

Descrizione: fornisce l'accesso completo a tutte le Amazon Route 53 tramite Console di gestione AWS.

`AmazonRoute53FullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistributionTenantByDomain",
        "cloudfront:GetConnectionGroup",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "es:ListDomainNames",
        "es:DescribeDomains",
        "lightsail:GetContainerServices",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53GlobalResolverFullAccess

Descrizione: Fornisce l'accesso completo per recuperare, elencare, creare, aggiornare ed eliminare tutte le risorse di Amazon Route 53 Global Resolver.

`AmazonRoute53GlobalResolverFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53GlobalResolverFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 marzo 2026, 20:27 UTC
- Ora modificata: 09 marzo 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53GlobalResolverFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53GlobalResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53globalresolver:AllowVendedLogDeliveryForResource",
        "route53globalresolver:AssociateHostedZone",
        "route53globalresolver:BatchCreateFirewallRule",
        "route53globalresolver:BatchDeleteFirewallRule",
        "route53globalresolver:BatchUpdateFirewallRule",
        "route53globalresolver:CreateAccessSource",
        "route53globalresolver:CreateAccessToken",
        "route53globalresolver:CreateDNSView",
        "route53globalresolver:CreateFirewallDomainList",
        "route53globalresolver:CreateFirewallRule",
        "route53globalresolver:CreateGlobalResolver",
        "route53globalresolver:DeleteAccessSource",
        "route53globalresolver:DeleteAccessToken",
        "route53globalresolver:DeleteDNSView",
        "route53globalresolver:DeleteFirewallDomainList",
        "route53globalresolver:DeleteFirewallRule",
        "route53globalresolver:DeleteGlobalResolver",
        "route53globalresolver:DisableDNSView",
        "route53globalresolver:DisassociateHostedZone",
        "route53globalresolver:EnableDNSView",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetAccessToken",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
```

```
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ImportFirewallDomains",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListManagedFirewallDomainLists",
        "route53globalresolver:ListTagsForResource",
        "route53globalresolver:TagResource",
        "route53globalresolver:UntagResource",
        "route53globalresolver:UpdateAccessSource",
        "route53globalresolver:UpdateAccessToken",
        "route53globalresolver:UpdateDNSView",
        "route53globalresolver:UpdateFirewallDomains",
        "route53globalresolver:UpdateFirewallRule",
        "route53globalresolver:UpdateGlobalResolver",
        "route53globalresolver:UpdateHostedZoneAssociation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53GlobalResolverReadOnlyAccess

Descrizione: fornisce accesso in sola lettura per recuperare ed elencare tutte le risorse di Amazon Route 53 Global Resolver.

`AmazonRoute53GlobalResolverReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53GlobalResolverReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 marzo 2026, 20:27 UTC
- Ora modificata: 09 marzo 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53GlobalResolverReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53GlobalResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetAccessToken",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
```

```
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListManagedFirewallDomainLists"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53ProfilesFullAccess

Descrizione: questa politica garantisce l'accesso completo alle risorse del profilo Amazon Route 53.

`AmazonRoute53ProfilesFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53ProfilesFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 aprile 2024, 18:30 UTC
- Ora modificata: 27 agosto 2024, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:AssociateProfile",
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:CreateProfile",
        "route53profiles:DeleteProfile",
        "route53profiles:DisassociateProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53profiles:PutProfilePolicy",
        "route53profiles:TagResource",
        "route53profiles:UntagResource",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverRule",
        "ec2:DescribeVpcs",
        "route53:GetHostedZone"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53ProfilesReadOnlyAccess

Descrizione: questa policy garantisce l'accesso in sola lettura alle risorse del profilo Amazon Route 53.

`AmazonRoute53ProfilesReadOnlyAccess`è una policy gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53ProfilesReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 aprile 2024, 18:29 UTC
- Ora modificata: 27 agosto 2024, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53ReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutte le Amazon Route 53 tramite Console di gestione AWS.

`AmazonRoute53ReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53ReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 15 novembre 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53RecoveryClusterFullAccess

Descrizione: Fornisce accesso completo ad Amazon Route 53 Recovery Cluster

`AmazonRoute53RecoveryClusterFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53RecoveryClusterFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2021, 18:37 UTC
- Ora modificata: 18 agosto 2021, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53RecoveryClusterReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon Route 53 Recovery Cluster

`AmazonRoute53RecoveryClusterReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53RecoveryClusterReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2021, 17:36 UTC
- Ora modificata: 01 aprile 2022, 17:37 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53RecoveryControlConfigFullAccess

Descrizione: Fornisce accesso completo ad Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53RecoveryControlConfigFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2021, 17:48 UTC
- Ora modificata: 18 agosto 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53RecoveryControlConfigReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53RecoveryControlConfigReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2021, 18:01 UTC
- Ora modificata: 18 ottobre 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeRoutingControlByName",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53RecoveryReadinessFullAccess

Descrizione: Fornisce accesso completo ad Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53RecoveryReadinessFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 18 agosto 2021, 16:45 UTC
- Ora modificata: 18 agosto 2021, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53RecoveryReadinessReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53RecoveryReadinessReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2021, 18:11 UTC
- Ora modificata: 09 novembre 2021, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
```

```
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListRules",
        "route53-recovery-readiness:ListTagsForResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
        "route53-recovery-readiness:GetCellReadinessSummary"
      ],
      "Resource" : "arn:aws:route53-recovery-readiness::*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53ResolverFullAccess

Descrizione: Politica di accesso completo per Route 53 Resolver

`AmazonRoute53ResolverFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53ResolverFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 maggio 2019, 18:10 UTC

- Ora modificata: 5 agosto 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonRoute53ResolverReadOnlyAccess

Descrizione: Politica di sola lettura per Route 53 Resolver

`AmazonRoute53ResolverReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonRoute53ResolverReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 maggio 2019, 18:11 UTC
- Ora modificata: 5 agosto 2024, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverReadOnlyAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3ExpressFullAccess

Descrizione: fornisce l'accesso completo a tutti i bucket di directory S3.

`AmazonS3ExpressFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3ExpressFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 aprile 2026, 20:42 UTC
- Ora modificata: 03 aprile 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ExpressFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3ExpressFullAccess",
      "Effect" : "Allow",
      "Action" : "s3express:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3ExpressReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle operazioni di S3Express per i bucket di directory S3.

`AmazonS3ExpressReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonS3ExpressReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 aprile 2026, 20:42 UTC
- Ora modificata: 03 aprile 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ExpressReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3ExpressReadOnlySessionObjectAccess",
      "Effect" : "Allow",
      "Action" : "s3express:CreateSession",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3express:SessionMode" : "ReadOnly"
        }
      }
    },
    {
      "Sid" : "S3ExpressReadOnlyControlPlaneAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
```

```
        "s3express:GetAccessPointScope",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3FilesClientFullAccess

Descrizione: fornisce l'accesso del client root a un file system S3 Files.

`AmazonS3FilesClientFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3FilesClientFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 aprile 2026, 12:57 UTC
- Ora modificata: 07 aprile 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount",
        "s3files:ClientWrite",
        "s3files:ClientRootAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3FilesClientReadOnlyAccess

Descrizione: fornisce l'accesso client in sola lettura a un file system S3 Files.

`AmazonS3FilesClientReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3FilesClientReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 aprile 2026, 12:57 UTC
- Ora modificata: 07 aprile 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3FilesClientReadWriteAccess

Descrizione: fornisce l'accesso client di lettura e scrittura a un file system S3 Files.

`AmazonS3FilesClientReadWriteAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3FilesClientReadWriteAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 aprile 2026, 12:57 UTC
- Ora modificata: 07 aprile 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientReadWriteAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount",
        "s3files:ClientWrite"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3FilesCSIDriverPolicy

Descrizione: Fornisce l'accesso di gestione alle risorse di Amazon S3 Files

`AmazonS3FilesCSIDriverPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3FilesCSIDriverPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 aprile 2026, 13:12 UTC
- Ora modificata: 07 aprile 2026, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3FilesCSIDriverPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowList",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "s3files:CreateAccessPoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowTagNewAccessPoints",
      "Effect" : "Allow",
      "Action" : [
        "s3files:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3files:CreateAction" : "CreateAccessPoint"
        },
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
```

```
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowDeleteAccessPoint",
      "Effect" : "Allow",
      "Action" : "s3files:DeleteAccessPoint",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3FilesFullAccess

Descrizione: fornisce l'accesso completo a tutti i file S3 tramite. Console di gestione AWS

`AmazonS3FilesFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3FilesFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 7 aprile 2026, 12:42 UTC
- Ora modificata: 07 aprile 2026, 12:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : "s3files:*",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2NetworkingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "EventBridgeManage",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "elasticfilesystem.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-S3-Files*"
      ]
    },
    {
      "Sid" : "EventBridgeRead",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListRules",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*"
      ]
    },
    {
      "Sid" : "IAMPassRoleForS3Files",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "elasticfilesystem.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3FilesReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutti i file S3 tramite. Console di gestione AWS

`AmazonS3FilesReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3FilesReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 aprile 2026, 12:57 UTC
- Ora modificata: 07 aprile 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:Get*",
        "s3files:List*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3FullAccess

Descrizione: fornisce l'accesso completo a tutti i bucket tramite. Console di gestione AWS

`AmazonS3FullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 27 settembre 2021, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3ObjectLambdaExecutionRolePolicy

Descrizione: fornisce le autorizzazioni per le funzioni AWS Lambda per interagire con Amazon S3 Object Lambda. Concede inoltre le autorizzazioni Lambda per la scrittura nei registri. CloudWatch

`AmazonS3ObjectLambdaExecutionRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonS3ObjectLambdaExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 18 agosto 2021, 10:07 UTC
- Ora modificata: 18 agosto 2021, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3OutpostsFullAccess

Descrizione: fornisce l'accesso completo ad Amazon S3 on Outposts tramite. Console di gestione AWS

`AmazonS3OutpostsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3OutpostsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 2 ottobre 2020, 17:26 UTC
- Ora modificata: 2 ottobre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3-outposts:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3OutpostsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon S3 on Outposts tramite. Console di gestione AWS

`AmazonS3OutpostsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3OutpostsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 ottobre 2020, 18:55 UTC
- Ora modificata: 2 ottobre 2020, 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3-outposts:Get*",
        "s3-outposts:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3ReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutti i bucket tramite. Console di gestione AWS

`AmazonS3ReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3ReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 10 agosto 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3TablesFullAccess

Descrizione: fornisce l'accesso completo a tutti i table bucket S3.

`AmazonS3TablesFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3TablesFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 dicembre 2024, 15:21 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToS3TablesReplication",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "replication.s3tables.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3TablesLakeFormationServiceRole

Descrizione: questa politica gestita concede a AWS Lake Formation le autorizzazioni per agire su tutti i table bucket, i namespace e le tabelle all'interno dell'account.

`AmazonS3TablesLakeFormationServiceRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonS3TablesLakeFormationServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 giugno 2025, 19:07 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3TablesLakeFormationServiceRole`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForS3ListTableBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:ListTableBuckets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:GetTableBucket",
        "s3tables:CreateNamespace",
        "s3tables:GetNamespace",
        "s3tables:ListNamespaces",
        "s3tables:DeleteNamespace",
        "s3tables:DeleteTableBucket",
        "s3tables:CreateTable",
        "s3tables:DeleteTable",
        "s3tables:GetTable",
        "s3tables:ListTables",
        "s3tables:RenameTable",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTableData",
```

```
        "s3tables:PutTableData",
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3tables:*:*:bucket/*/table/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDescribeKeyAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3tables.*.amazonaws.com"
          ]
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonS3TablesReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a tutti i table bucket S3.

`AmazonS3TablesReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonS3TablesReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 dicembre 2024, 15:21 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:Get*",
        "s3tables:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata dal servizio Servizio AWS Catalog per fornire prodotti del SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a una serie di servizi correlati tra cui CodePipeline, CodeBuild,, CodeCommit Glue CloudFormation, ecc.

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2020, 18:48 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPostPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPatchPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PATCH"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnMutatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "ArnLikeIfExists" : {
          "cloudformation:RoleArn" : [
            "arn:aws:sts::*:assumed-role/AmazonSageMakerServiceCatalog*"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTemplatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*"
      ]
```

```
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateCommit",
        "codecommit:CreateRepository",
        "codecommit:DeleteRepository",
        "codecommit:GetRepository",
        "codecommit:TagResource"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitListPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodePipelinePermission",
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline:DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
      ],
      "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMUserPermission",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateUserPool",
```

```
        "cognito-idp:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DeleteUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
```

```
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogFirehosePermission",
      "Effect" : "Allow",
      "Action" : [
        "firehose:CreateDeliveryStream",
        "firehose:DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGluePermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
      ]
```

```
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueClassiferPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateClassifier",
        "glue:DeleteClassifier",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeleteTrigger",
        "glue:DeleteWorkflow",
        "glue:StopCrawler"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueWorkflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateWorkflow"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:workflow/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueJobPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:job/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueCrawlerPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:GetCrawler"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:crawler/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueTriggerPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTrigger",
        "glue:GetTrigger"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:trigger/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaTagPermission",
      "Effect" : "Allow",
```

```
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
        "arn:aws:logs:*:*:log-group::log-stream:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadPermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadSagemakerResourcePermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
```

```
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3MutatePermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketTagging",
        "s3:PutObjectTagging"
      ],
      "Resource" : "arn:aws:s3:::sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeWorkteam",
        "sagemaker:CreateCodeRepository",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:DeleteCodeRepository"
```

```
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateImage",
        "sagemaker:DeleteImage",
        "sagemaker:DescribeImage",
        "sagemaker:UpdateImage",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:image/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogStepFunctionPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "states:CreateStateMachine",
        "states:DeleteStateMachine",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeStarPermission",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerCanvasAIServicesAccess

Descrizione: fornisce le autorizzazioni ad Amazon SageMaker Canvas per utilizzare i servizi di intelligenza artificiale per supportare soluzioni AI pronte all'uso. Questa politica aggiungerà ulteriori autorizzazioni mutanti per i servizi man mano che Amazon SageMaker Canvas aggiungerà il supporto.

`AmazonSageMakerCanvasAIServicesAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerCanvasAIServicesAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 marzo 2023, 22:36 UTC
- Ora modificata: 29 novembre 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "Textract",
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument",
        "textract:AnalyzeExpense",
        "textract:AnalyzeID",
        "textract:StartDocumentAnalysis",
        "textract:StartExpenseAnalysis",
        "textract:GetDocumentAnalysis",
        "textract:GetExpenseAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Rekognition",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectLabels",
        "rekognition:DetectText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Comprehend",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:BatchDetectEntities",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectPiiEntities",
        "comprehend:DetectEntities",
        "comprehend:DetectSentiment",
        "comprehend:DetectDominantLanguage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:InvokeModelWithResponseStream"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker",
            "Canvas"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:RequestTag/Canvas" : "true",
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
    },
    {
      "Sid" : "GetStopAndDeleteBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetCustomModel",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:StopModelCustomizationJob",
        "bedrock:DeleteProvisionedModelThroughput"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
```

```
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
    },
    {
      "Sid" : "FoundationModelPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "BedrockFineTuningPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerCanvasBedrockAccess

Descrizione: questa politica concede le autorizzazioni per utilizzare Amazon Bedrock in SageMaker Canvas fornendo l'accesso a servizi downstream come S3.

`AmazonSageMakerCanvasBedrockAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerCanvasBedrockAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 febbraio 2024, 18:37 UTC
- Ora modificata: 02 febbraio 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3CanvasAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas",
        "arn:aws:s3:::sagemaker-*/Canvas/*"
      ]
    },
    {
      "Sid" : "S3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerCanvasDataPrepFullAccess

Descrizione: fornisce l'accesso completo alle SageMaker risorse e alle operazioni di Amazon per la preparazione dei dati in Canvas. La policy fornisce anche un accesso selezionato ai servizi correlati (ad esempio, S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena, Glue, Secrets Manager). EventBridge Questa policy deve essere allegata al ruolo di esecuzione Amazon SageMaker Domain/ User Profile.

`AmazonSageMakerCanvasDataPrepFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerCanvasDataPrepFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 ottobre 2023, 22:56 UTC
- Ora modificata: 16 agosto 2024, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerListFeatureGroupOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListFeatureGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerFeatureGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateFeatureGroup",
        "sagemaker:DescribeFeatureGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
    },
    {
      "Sid" : "SageMakerProcessingJobOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateProcessingJob",
```

```
        "sagemaker:DescribeProcessingJob",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
    },
    {
      "Sid" : "SageMakerProcessingJobListOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListProcessingJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPipelineOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribePipeline",
        "sagemaker:CreatePipeline",
        "sagemaker:UpdatePipeline",
        "sagemaker:DeletePipeline",
        "sagemaker:StartPipelineExecution",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:DescribePipelineExecution"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
    },
    {
      "Sid" : "KMSListOperations",
      "Effect" : "Allow",
      "Action" : "kms:ListAliases",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
```

```
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListOperations",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgePutOperation",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "EMROperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups"
```

```
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
    },
    {
      "Sid" : "EMRListOperation",
      "Effect" : "Allow",
      "Action" : "elasticmapreduce:ListClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaListDataCatalogOperation",
      "Effect" : "Allow",
      "Action" : "athena:ListDataCatalogs",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaQueryExecutionOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*"
    },
    {
      "Sid" : "AthenaDataCatalogOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*"
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "RedshiftArnBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "arn:aws:redshift:*:*:cluster:*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
```

```
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:GetApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerCanvasDirectDeployAccess

Descrizione: consente ad Amazon SageMaker Canvas di creare, gestire e visualizzare i dettagli degli endpoint per gli endpoint creati tramite Canvas. Consente ad Amazon SageMaker Canvas di recuperare i parametri di chiamata degli endpoint da. CloudWatch

`AmazonSageMakerCanvasDirectDeployAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerCanvasDirectDeployAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 ottobre 2023, 18:11 UTC
- Ora modificata: 6 ottobre 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerEndpointPerms",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:Canvas*",
        "arn:aws:sagemaker:*:*:canvas*"
      ]
    },
    {
      "Sid" : "ReadCWInvocationMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy

Descrizione: questa politica concede le autorizzazioni ad Amazon EMR Serverless per servizi come S3, utilizzati da SageMaker Amazon Canvas per l'elaborazione di dati di grandi dimensioni.

`AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 luglio 2024, 00:35 UTC
- Ora modificata: 27 luglio 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerCanvasForecastAccess

Descrizione: questa politica concede le autorizzazioni comunemente necessarie per utilizzare SageMaker Canvas con Amazon Forecast.

`AmazonSageMakerCanvasForecastAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerCanvasForecastAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 24 agosto 2022, 20:04 UTC
- Ora modificata: 24 agosto 2022, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas*",
```

```
        "arn:aws:s3:::sagemaker-*/canvas*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerCanvasFullAccess

Descrizione: fornisce l'accesso completo alle risorse e alle operazioni di Amazon SageMaker Canvas. La policy fornisce anche un accesso selezionato ai servizi correlati (ad esempio, S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager e Forecast). Questa policy deve essere allegata al ruolo di esecuzione Amazon SageMaker Domain/User Profile.

`AmazonSageMakerCanvasFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerCanvasFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 09 settembre 2022, 00:44 UTC

- Ora modificata: 16 agosto 2024, 04:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPackageGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
```

```
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:AddTags",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*",
        "arn:aws:sagemaker:*:*:*model-compilation-*"
      ]
    },
    {
      "Sid" : "SageMakerHostingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:InvokeEndpoint",
```

```
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:InvokeEndpointAsync"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*"
      ]
    },
    {
      "Sid" : "EC2VPCOperation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECROperations",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:GetBucketCors",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
```

```
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : "glue:SearchTables",
      "Resource" : [
        "arn:aws:glue:*:*:table/*/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
```

```
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassOperationForForecast",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AutoscalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "application-autoscaling:scalable-dimension" :
"sagemaker:variant:DesiredInstanceCount"
        }
      }
    },
    {
      "Sid" : "AsyncEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "sagemaker:DescribeEndpointConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeScalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
```

```
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingSageMakerEndpointOperation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AthenaOperation",
      "Action" : [
        "athena:ListTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueOperation",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTables"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuicksightOperation",
      "Action" : [
        "quicksight:ListNamespaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUseOfKeyInAccount",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Source" : "SageMakerCanvas",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
```

```
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerCanvasSMDataScienceAssistantAccess

Descrizione: fornisce le autorizzazioni per Amazon SageMaker Canvas per utilizzare il servizio SageMaker Data Science Assistant. Attualmente Data Science Assistant utilizza sia Amazon che Amazon SageMaker Q Developer per elaborare le richieste degli utenti.

`AmazonSageMakerCanvasSMDataScienceAssistantAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerCanvasSMDataScienceAssistantAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 4 dicembre 2024, 14:06 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasSMDataScienceAssistantAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerDataScienceAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-data-science-assistant:SendConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerCapacityReservationServiceRolePolicy

Descrizione: questa politica concede le autorizzazioni ad Amazon SageMaker Capacity Reservations per pubblicare CloudWatch metriche negli account dei clienti per la visibilità dell'utilizzo.

`AmazonSageMakerCapacityReservationServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 8 aprile 2026, 20:27 UTC
- Ora modificata: 08 aprile 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCapacityReservationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchPutMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "aws/sagemaker/CapacityReservations"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerClusterInstanceRolePolicy

Descrizione: questa politica concede le autorizzazioni comunemente necessarie per utilizzare Amazon SageMaker Cluster.

`AmazonSageMakerClusterInstanceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerClusterInstanceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2023, 15:11 UTC
- Ora modificata: 29 novembre 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchLogStreamPublishPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudwatchLogGroupCreationPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*"
      ]
    },
    {
      "Sid" : "CloudwatchPutMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/sagemaker/Clusters"
        }
      }
    },
    {
      "Sid" : "DataRetrievalFromS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMConnectivityPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
```

```
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerCoreServiceRolePolicy

Descrizione: policy gestita per Service Linked Role for Amazon SageMaker Core Services

`AmazonSageMakerCoreServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 dicembre 2020, 21:40 UTC
- Ora modificata: 21 dicembre 2020, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:AuthorizedService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerEdgeDeviceFleetPolicy

Descrizione: fornisce le autorizzazioni necessarie a SageMaker Edge per creare e gestire una flotta di dispositivi per il cliente utilizzando la connessione cloud predefinita.

`AmazonSageMakerEdgeDeviceFleetPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerEdgeDeviceFleetPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 08 dicembre 2020, 16:17 UTC
- Ora modificata: 08 dicembre 2020, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "SageMakerEdgeApis",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SendHeartbeat",
        "sagemaker:GetDeviceRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateIoTRoleAlias",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateRoleAlias",
        "iot:DescribeRoleAlias",
        "iot:UpdateRoleAlias",
        "iot:ListTagsForResource",
        "iot:TagResource"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:rolealias/SageMakerEdge*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "credentials.iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerFeatureStoreAccess

Descrizione: fornisce le autorizzazioni necessarie per abilitare lo store offline per un gruppo di SageMaker FeatureStore funzionalità Amazon.

`AmazonSageMakerFeatureStoreAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerFeatureStoreAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2020, 16:24 UTC
- Ora modificata: 05 dicembre 2022, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*/metadata/*",
        "arn:aws:s3:::*Sagemaker*/metadata/*",
        "arn:aws:s3:::*sagemaker*/metadata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerFullAccess

Descrizione: fornisce l'accesso completo ad Amazon SageMaker tramite l'SDK Console di gestione AWS and. Fornisce inoltre un accesso selezionato ai servizi correlati (ad esempio, S3, ECR, CloudWatch Logs).

`AmazonSageMakerFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 13:07 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Versione della politica

Versione della politica: v29 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:partner-app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*",
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
```

```
      ]
    },
    {
      "Sid" : "AllowAddTagsForSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    },
    {
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*"
      ]
    },
    {
      "Sid" : "AllowUseOfTrainingPlanResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateCluster",
        "sagemaker:UpdateCluster",
        "sagemaker:DescribeTrainingPlan"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:DescribeSpace",
        "sagemaker:ListSpaces",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
```

```
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
```

```
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:List*",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
```

```
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "glue:CreateJob",
        "glue:DeleteJob",
        "glue:GetJob*",
        "glue:GetTable*",
        "glue:GetWorkflowRun",
        "glue:ResetJobBookmark",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
```

```
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
```

```
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
```

```
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
```

```
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
    },
    {
      "Sid" : "AllowGlueDeleteTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
```

```
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
```

```
        "arn:aws:s3express:*:*:bucket/*aws-glue*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressCreateBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressListBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:ListAllMyDirectoryBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerGeospatialExecutionRole

Descrizione: questa politica fornisce l'accesso ai servizi che sono comunemente necessari per l'uso della tecnologia SageMaker geospaziale.

`AmazonSageMakerGeospatialExecutionRole`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerGeospatialExecutionRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 30 novembre 2022, 10:08 UTC
- Ora modificata: 10 maggio 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
```

```
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetEarthObservationJob",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:earth-observation-job/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetRasterDataCollection",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:raster-data-collection/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerGeospatialFullAccess

Descrizione: questa politica concede autorizzazioni che consentono l'accesso completo ad Amazon SageMaker Geospatial tramite l'SDK and. Console di gestione AWS

`AmazonSageMakerGeospatialFullAccess`AWS è una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerGeospatialFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 30 novembre 2022, 10:06 UTC
- Ora modificata: 30 novembre 2022, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker-geospatial.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerGroundTruthExecution

Descrizione: fornisce l'accesso ai AWS servizi necessari per eseguire il processo di SageMaker GroundTruth etichettatura

`AmazonSageMakerGroundTruthExecution`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerGroundTruthExecution` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 luglio 2020, 19:30 UTC
- Ora modificata: 29 aprile 2022, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CustomLabelingJobs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*GtRecipe*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*",
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*GroundTruth*",
        "arn:aws:s3:::*Groundtruth*",
        "arn:aws:s3:::*groundtruth*",
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
```

```
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StreamingQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:*GroundTruth*"
    },
    {
      "Sid" : "StreamingTopicSubscribe",
      "Effect" : "Allow",
      "Action" : "sns:Subscribe",
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
```

```
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sns:Protocol" : "sqs"
        },
        "StringLike" : {
          "sns:Endpoint" : "arn:aws:sqs:*:*:*GroundTruth*"
        }
      }
    },
    {
      "Sid" : "StreamingTopic",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "StreamingTopicUnsubscribe",
      "Effect" : "Allow",
      "Action" : [
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WorkforceVPC",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ec2:VpceServiceName" : [
            "*sagemaker-task-resources*",
            "aws.sagemaker*labeling*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerHyperPodGatedModelAccess

Descrizione: questa Amazon Managed Policy fornisce le autorizzazioni necessarie per accedere SageMaker HyperPod ai modelli controllati in SageMaker Jumpstart. Consente di creare contenuti predefiniti URLs per l'hub nel Public Hub. SageMaker

`AmazonSageMakerHyperPodGatedModelAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerHyperPodGatedModelAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 gennaio 2026, 01:04 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodGatedModelAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreatePresignedUrlAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateHubContentPresignedUrls"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:hub/SageMakerPublicHub",
        "arn:aws:sagemaker:*:*:hub-content/SageMakerPublicHub/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerHyperPodInferenceAccess

Descrizione: questa politica fornisce i privilegi amministrativi necessari per impostare l'operatore di SageMaker HyperPod inferenza. Consente all'operatore di inferenza di accedere alle risorse AWS di rete, Amazon S3, Amazon ECR, Amazon CloudWatch, AWS Certificate Manager e alle SageMaker risorse necessarie per distribuire e gestire i carichi di lavoro di inferenza sui cluster HyperPod

`AmazonSageMakerHyperPodInferenceAccess`AWS è una policy gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerHyperPodInferenceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 gennaio 2026, 20:34 UTC
- Ora modificata: 20 luglio 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodInferenceAccess`

Versione della politica

Versione della politica: v4 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteObjectsPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "s3:ExistingObjectTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "S3PutObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectTagging"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "s3:RequestObjectTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "DataCaptureS3",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/data-capture/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListBucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataCaptureKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com",
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::hyperpod-tls*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRAuthorization",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRRepositoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "EC2DescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "EC2NetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EKSClusterAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EKSAccessEntryPolicyAssociation",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "eks:policyarn" : "arn:aws:eks::aws:cluster-access-policy/
AmazonSagemakerHyperpodInferenceMonitoringPolicy"
        }
      }
    },
    {
      "Sid" : "EKSAccessEntryListPolicies",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ELBListAndDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FSxAccess",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "CertificateImportPermission",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:ImportCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CreatedBy"
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CertificateDeletePermission",
      "Effect" : "Allow",
      "Action" : "acm:DeleteCertificate",
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerHyperPodInference*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "CloudWatchMetricsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterInference",
        "sagemaker:UpdateClusterInference",
        "sagemaker:DescribeHubContent"
      ],
```

```
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpointconfig/*",
        "arn:aws:sagemaker:*:*:cluster/*",
        "arn:aws:sagemaker:*:*:hub-content/*",
        "arn:aws:sagemaker:*:*:hub/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModel",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "SageMakerTagging",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateModel",
            "CreateEndpointConfig",
            "CreateEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerDeleteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteModel",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "HyperPodInference"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerHyperPodObservabilityAdminAccess

Descrizione: questa politica fornisce i privilegi amministrativi necessari per impostare l' SageMaker HyperPod osservabilità. Consente l'accesso ad Amazon Managed Prometheus, Amazon Managed Grafana ed EKS Addons. La policy include anche un ampio accesso a Grafana HTTP APIs ServiceAccountTokens attraverso tutte le aree di lavoro Amazon Managed Grafana del tuo account.

`AmazonSageMakerHyperPodObservabilityAdminAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerHyperPodObservabilityAdminAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 luglio 2025, 14:37 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodObservabilityAdminAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrometheusCreateAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aps:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusTagsAccess",
      "Effect" : "Allow",
      "Action" : "aps:TagResource",
      "Resource" : [
        "arn:aws:aps:*:*:/workspaces",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:DescribeWorkspace"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*"
    },
    {
      "Sid" : "PrometheusListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:ListWorkspaces"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "PrometheusAlertsRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateAlertManagerDefinition",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces"
      ],
      "Resource" : [
        "arn:aws:aps:*:*:workspace/*",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ]
    },
    {
      "Sid" : "PrometheusCreateRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : "aps:CreateRuleGroupsNamespace",
      "Resource" : "arn:aws:aps:*:*:rulegroupsnamespace/*/
HyperPodObservabilityNamespace",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaCreateWorkspaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaTagsAccess",
      "Effect" : "Allow",
```

```
      "Action" : "grafana:TagResource",
      "Resource" : "arn:aws:grafana:*:*:/workspaces",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaListAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:ListWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaServiceAccountAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:CreateWorkspaceApiKey",
        "grafana:CreateWorkspaceServiceAccount",
        "grafana:CreateWorkspaceServiceAccountToken",
        "grafana:ListWorkspaceServiceAccounts",
        "grafana:ListWorkspaceServiceAccountTokens",
        "grafana:DeleteWorkspaceServiceAccountToken"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces/*"
    },
    {
      "Sid" : "IAMGrafanaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityGrafanaAccess-*",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "grafana.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMEKSPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*"
      ]
    },
    {
      "Sid" : "HyperPodClusterAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListClusters",
        "sagemaker:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/amazon-sagemaker-hyperpod-observability/*"
    },
    {
      "Sid" : "EKSAddonDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeAddonConfiguration",
        "eks:DescribeAddonVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonPodIdentityAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribePodIdentityAssociation",
        "eks:DeletePodIdentityAssociation",
        "eks:UpdatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSListDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAddons",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "EKSCreateAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "eks:CreateAddon",
        "eks:CreatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSTagsAccess",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:addon/*/*/*",
        "arn:aws:eks:*:*:podidentityassociation/*/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "SSOAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:CreateManagedApplicationInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerHyperPodServiceRolePolicy

Descrizione: questa politica concede le autorizzazioni SageMaker HyperPod ad Amazon per AWS servizi correlati come Amazon EKS, Amazon ecc. CloudWatch

`AmazonSageMakerHyperPodServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 6 settembre 2024, 17:04 UTC
- Ora modificata: 6 settembre 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerHyperPodServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EKSClusterDescribePermissions",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogStreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerHyperPodTrainingOperatorAccess

Descrizione: questa politica fornisce le autorizzazioni amministrative necessarie per configurare l'operatore di SageMaker HyperPod formazione. Consente l'accesso ai componenti aggiuntivi Amazon SageMaker HyperPod ed EKS. La politica include le autorizzazioni per descrivere SageMaker HyperPod le risorse del tuo account.

`AmazonSageMakerHyperPodTrainingOperatorAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerHyperPodTrainingOperatorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 agosto 2025, 17:04 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodTrainingOperatorAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeClusterNodeOnHyperPodClusters",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeClusterNode",
      "Resource" : "arn:aws:sagemaker:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerInferenceServiceRolePolicy

Descrizione: politica gestita per Service Linked Role for Amazon SageMaker Inference.

`AmazonSageMakerInferenceServiceRolePolicy`è una policy AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 30 luglio 2026, 19:42 UTC
- Ora modificata: 30 luglio 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerInferenceServiceRolePolicy`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateENIWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "CreateENIInSubnetAndSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "CreateENIPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:AuthorizedService" : "sagemaker.amazonaws.com",
          "ec2:Permission" : "INSTANCE-ATTACH",
          "aws:ResourceTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "DeleteENITagScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "DeleteENIPermissionTagScoped",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "TagOnCreateSageMakerResourcesForENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:RequestTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerJobFullAccess

Descrizione: fornisce le autorizzazioni per i ruoli di esecuzione di SageMaker lavori di Amazon per accedere ai dati in Amazon S3, richiamare agenti tramite Amazon AgentCore Bedrock, tenere traccia degli esperimenti con MLFlow, pubblicare pacchetti di modelli, scrivere log su Amazon CloudWatch, richiamare AWS funzioni Lambda e gestire le interfacce di rete Amazon VPC.

`AmazonSageMakerJobFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerJobFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 giugno 2026, 02:42 UTC
- Ora modificata: 03 giugno 2026, 02:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerJobFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:hub/*",
        "arn:aws:sagemaker:*:*:hub-content/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerModelPackagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AccessModelPackage",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MLflowPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:DescribeMlflowApp",
        "sagemaker:CallMlflowAppApi",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:UpdateRun",
        "sagemaker-mlflow:LogBatch",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:StartTrace",
        "sagemaker-mlflow:EndTrace",
        "sagemaker-mlflow:SearchTraces",
        "sagemaker-mlflow:ListArtifacts"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:InvokeAgentRuntime",
        "bedrock-agentcore:StopRuntimeSession",
        "bedrock-agentcore:GetAgentRuntime"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:runtime/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2NetworkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeDhcpOptions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2NetworkInterfaceTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "EC2NetworkInterfaceDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerJobRuntimeAccess

Descrizione: fornisce le autorizzazioni per i runtime degli agenti per richiamare le API di Amazon SageMaker Job Runtime utilizzate durante la personalizzazione del modello per la generazione di campioni, il completamento della traiettoria e l'invio di ricompense.

`AmazonSageMakerJobRuntimeAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerJobRuntimeAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 giugno 2026, 02:42 UTC
- Ora modificata: 03 giugno 2026, 02:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerJobRuntimeAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerJobRuntimePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Sample",
```

```
        "sagemaker:SampleWithResponseStream",
        "sagemaker:CompleteRollout",
        "sagemaker:UpdateReward"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:job/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BearerTokenPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CallWithBearerToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerMechanicalTurkAccess

Descrizione: fornisce l'accesso per creare risorse Amazon Augmented FlowDefinition AI per qualsiasi team di lavoro.

`AmazonSageMakerMechanicalTurkAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerMechanicalTurkAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 16:19 UTC
- Ora modificata: 03 dicembre 2019, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerModelCustomizationCoreAccess

Descrizione: concede le autorizzazioni per i flussi di lavoro di personalizzazione SageMaker del modello, tra cui formazione senza server, funzione di ricompensa personalizzata per il reinforcement learning, valutazione del modello e distribuzione sui nostri endpoint Bedrock. SageMaker

`AmazonSageMakerModelCustomizationCoreAccess`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerModelCustomizationCoreAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 maggio 2026, 18:57 UTC
- Ora modificata: 21 luglio 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelCustomizationCoreAccess`

Versione della politica

Versione della politica: v3 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerPublicHubPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "SageMakerHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ImportHubContent",
        "sagemaker:ListHubs",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubContentVersions",
        "sagemaker:DescribeHubContent",
        "sagemaker:DeleteHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:hub/*",
        "arn:aws:sagemaker:*:*:hub-content/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "JumpStartS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::jumpstart*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingJob",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListTrainingJobs",
        "sagemaker:StopTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerMLFlow",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateMlflowApp",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:CreatePresignedMlflowAppUrl",
        "sagemaker:CallMlflowAppApi",
        "sagemaker-mlflow:AccessUI",
        "sagemaker-mlflow:GetExperiment",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:GetLoggedModel",
        "sagemaker-mlflow:SearchExperiments",
        "sagemaker-mlflow:SearchRuns",
        "sagemaker-mlflow:ListArtifacts",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:LogBatch",
        "sagemaker-mlflow:LogMetric",
        "sagemaker-mlflow:LogParam",
        "sagemaker-mlflow:LogModel",
        "sagemaker-mlflow:LogInputs",
        "sagemaker-mlflow:SetTag",
        "sagemaker-mlflow:UpdateRun"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BYODataSetS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerModelPackage",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:DescribeModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-package/*",
```

```
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerLineage",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateAction",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateContext",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:QueryLineage",
        "sagemaker:AddAssociation",
        "sagemaker:UpdateArtifact"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:artifact/*",
        "arn:aws:sagemaker:*:*:context/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:pipeline/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerPipelines",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePipeline",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
```

```
        "sagemaker:DescribePipelineExecution",
        "sagemaker:UpdatePipeline",
        "sagemaker:StartPipelineExecution"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:pipeline/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerInference",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:DeleteEndpoint",
        "sagemaker:InvokeEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:inference-component/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerInferenceAutoscaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
      ],
```

```
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerInferenceEcrReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListActions",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListEndpoints",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListMlflowApps",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListWorkforces",
        "sagemaker:Search"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerTagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:hub/*",
        "arn:aws:sagemaker:*:*:hub-content/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:inference-component/*",
        "arn:aws:sagemaker:*:*:action/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerJobAdvancedSettings",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "CloudWatchLogReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/*",
        "arn:aws:logs:*:*:log-group::log-stream:"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaListFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPermissionsForRewardFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:InvokeFunction",
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaLayerForAWSSDK",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetLayerVersion"
      ],
      "Resource" : [
        "arn:aws:lambda:*:336392948345:layer:AWSSDK*"
      ]
    },
    {
      "Sid" : "BedrockCustomModelAndEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateCustomModel",
        "bedrock:CreateEvaluationJob",
        "bedrock:GetCustomModel",
        "bedrock:GetModelImportJob",
        "bedrock:GetImportedModel",
        "bedrock:GetEvaluationJob",
```

```
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:evaluation-job/*",
        "arn:aws:bedrock:*:*:imported-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:model-import-job/*",
        "arn:aws:bedrock:*:*:foundation-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockModelImportAndList",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelImportJob",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:ListCustomModelDeployments",
        "bedrock:ListCustomModels",
        "bedrock:ListModelImportJobs"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockFoundationModelOperations",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModelAvailability",
        "bedrock:ListFoundationModels"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "PassRoleForSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/*SageMaker*",
        "arn:aws:iam::*:role/service-role/*Sagemaker*",
        "arn:aws:iam::*:role/service-role/*sagemaker*"
      ],
      "Condition" : {
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:sagemaker:*:*:*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "job.sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForAWSLambda",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerForLambda*",
        "arn:aws:iam::*:role/service-role/SageMakerForLambda*"
      ],
      "Condition" : {
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:lambda:*:*:function:*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "PassRoleForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerForBedrock*",
        "arn:aws:iam::*:role/service-role/SageMakerForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerModelGovernanceUseAccess

Descrizione: questa politica AWS gestita concede le autorizzazioni necessarie per utilizzare tutte le funzionalità di Amazon SageMaker Governance. La policy fornisce anche un accesso selezionato ai servizi correlati (ad esempio, S3, KMS).

`AmazonSageMakerModelGovernanceUseAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerModelGovernanceUseAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2022, 08:58 UTC
- Ora modificata: 04 giugno 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSMMonitoringModelCards",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker:DeleteModelCard",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:CreateModelCardExportJob",
        "sagemaker:DescribeModelCardExportJob",
```

```
        "sagemaker:ListModelCardExportJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSMTrainingModelsSearchTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListModels",
        "sagemaker:DescribeModel",
        "sagemaker:Search",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "sagemaker:ListTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3Actions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:CreateBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowS3ListActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerModelRegistryFullAccess

Descrizione: Questa è una nuova politica gestita per Model Registry in Sagemaker. Questa politica è una politica autonoma che può essere associata al ruolo utente per accedere alle funzionalità relative al Model Registry in Sagemaker.

`AmazonSageMakerModelRegistryFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerModelRegistryFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 aprile 2023, 05:20 UTC
- Ora modificata: 6 giugno 2024, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAction",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceRecommendationsJob",
```

```
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:UpdateModelPackage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryS3GetPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryS3ListPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryTagReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "sagemaker:collection"
        }
      }
    },
```

```
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:collection" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerNotebooksServiceRolePolicy

Descrizione: policy gestita per Service Linked Role per Amazon SageMaker Notebooks

`AmazonSageMakerNotebooksServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 ottobre 2019, 20:27 UTC
- Ora modificata: 16 aprile 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFSxDescribe",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDeleteApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*"
    },
    {
      "Sid" : "AllowEFSAccessPointCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSAccessPointDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSMountWithDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEFSTagging",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:TagResource",
      "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
```

```
    {
      "Sid" : "AllowEC2Tagging",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowEC2Operations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2AuthZ",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
```

```
    },
    {
      "Sid" : "AllowIdcOperations",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso:DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "AllowSagemakerProfileCreation",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSagemakerSpaceOperationsForCanvasManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DescribeSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*"
    },
    {
      "Sid" : "AllowSagemakerAddTagsForAppManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerPartnerAppsFullAccess

Descrizione: consente agli utenti delle app SageMaker partner Amazon di accedere alle applicazioni, elencare le applicazioni disponibili, avviare applicazioni Web UIs e connettersi tramite l'SDK dell'applicazione.

`AmazonSageMakerPartnerAppsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerPartnerAppsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 gennaio 2025, 18:37 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerPartnerListAppsPermission",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListPartnerApps",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AmazonSageMakerPartnerAppsPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:DescribePartnerApp",
        "sagemaker:CallPartnerAppApi"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:sagemaker:*:*:partner-app/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

Descrizione: politica relativa al ruolo di servizio utilizzata all' AWS APIGateway interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni per una serie di servizi correlati, tra cui Lambda e altri.

`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 agosto 2023, 15:06 UTC
- Ora modificata: 01 agosto 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:sagemaker-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker:InvokeEndpoint",
      "Resource" : "arn:aws:sagemaker:*:*:endpoint/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

Descrizione: politica relativa al ruolo di servizio utilizzata all' AWS CloudFormation interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a un sottoinsieme di servizi correlati, tra cui Lambda e altri. APIGateway

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 agosto 2023, 15:06 UTC

- Ora modificata: 01 agosto 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsLambdaRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsApiGatewayRole"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "apigateway.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:ListTags",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PublishLayerVersion",
        "lambda:GetLayerVersion",
        "lambda:DeleteLayerVersion",
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:sagemaker-*",
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/tags/*"
```

```
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/lambda-auth-code/layer.zip"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

Descrizione: politica del ruolo di servizio utilizzata da AWS Lambda all'interno dei prodotti AWS ServiceCatalog forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a una serie di servizi correlati, tra cui Secrets Manager e altri.

`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 agosto 2023, 15:05 UTC
- Ora modificata: 01 agosto 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:partner" : false
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerPipelinesIntegrations

Descrizione: questa Amazon Managed Policy concede le autorizzazioni comunemente necessarie per l'uso con le fasi di Callback e le fasi Lambda in Model Building Pipelines. SageMaker Viene aggiunto al AmazonSageMaker - ExecutionRole che può essere creato durante la configurazione di Studio. SageMaker Può anche essere associato a qualsiasi altro ruolo che verrà utilizzato per la creazione o l'esecuzione di pipeline.

`AmazonSageMakerPipelinesIntegrations`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerPipelinesIntegrations` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 luglio 2021, 16:35 UTC

- Ora modificata: 17 febbraio 2023, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*sageMaker*",
        "arn:aws:lambda:*:*:function:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*sagemaker*",
        "arn:aws:sqs:*:*:*sageMaker*",
        "arn:aws:sqs:*:*:*SageMaker*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRStepStatusUpdateRule",
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRClusterStatusUpdateRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ]
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerQuickSightVPCPolicy

Descrizione: questa policy verrà utilizzata da SageMaker Unified Studios per creare risorse relative al VPC per QuickSight

`AmazonSageMakerQuickSightVPCPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerQuickSightVPCPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 3 giugno 2025, 17:37 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerQuickSightVPCPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageQuickSightVPCConnection",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListVPCConnections",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcconnection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeQuickSightVPCConnectionEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "ManageQuickSightEC2NetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon SageMaker tramite l'SDK Console di gestione AWS and.

`AmazonSageMakerReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 13:07 UTC
- Ora modificata: 01 dicembre 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:BatchGetMetrics",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:BatchGetRecord",
        "sagemaker:GetRecord",
        "sagemaker:Search",
        "sagemaker:QueryLineage",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:GetModelPackageGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "aws-marketplace:ViewSubscriptions",
        "cloudwatch:DescribeAlarms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "ecr:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

Descrizione: politica relativa al ruolo di servizio utilizzata all' AWS APIGateway interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni per una serie di servizi correlati, tra cui CloudWatch Logs e altri.

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 25 marzo 2022, 04:25 UTC
- Ora modificata: 25 marzo 2022, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
```

```
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apigateway/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

Descrizione: politica relativa al ruolo di servizio utilizzata all' AWS CloudFormation interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a un sottoinsieme di servizi correlati, inclusi altri. SageMaker

`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 25 marzo 2022, 04:26 UTC
- Ora modificata: 25 marzo 2022, 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
```

```
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
```

```
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
```

```
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
```

```
            "sagemaker:GetSearchSuggestions",
            "sagemaker:InvokeEndpoint",
            "sagemaker:InvokeEndpointAsync",
            "sagemaker:ListActions",
            "sagemaker:ListAlgorithms",
            "sagemaker:ListAppImageConfigs",
            "sagemaker:ListApps",
            "sagemaker:ListArtifacts",
            "sagemaker:ListAssociations",
            "sagemaker:ListAutoMLJobs",
            "sagemaker:ListCandidatesForAutoMLJob",
            "sagemaker:ListCodeRepositories",
            "sagemaker:ListCompilationJobs",
            "sagemaker:ListContexts",
            "sagemaker:ListDataQualityJobDefinitions",
            "sagemaker:ListDeviceFleets",
            "sagemaker:ListDevices",
            "sagemaker:ListDomains",
            "sagemaker:ListEdgePackagingJobs",
            "sagemaker:ListEndpointConfigs",
            "sagemaker:ListEndpoints",
            "sagemaker:ListExperiments",
            "sagemaker:ListFeatureGroups",
            "sagemaker:ListFlowDefinitions",
            "sagemaker:ListHumanLoops",
            "sagemaker:ListHumanTaskUis",
            "sagemaker:ListHyperParameterTuningJobs",
            "sagemaker:ListImageVersions",
            "sagemaker:ListImages",
            "sagemaker:ListInferenceRecommendationsJobs",
            "sagemaker:ListLabelingJobs",
            "sagemaker:ListLabelingJobsForWorkteam",
            "sagemaker:ListLineageGroups",
            "sagemaker:ListModelBiasJobDefinitions",
            "sagemaker:ListModelExplainabilityJobDefinitions",
            "sagemaker:ListModelMetadata",
            "sagemaker:ListModelPackageGroups",
            "sagemaker:ListModelPackages",
            "sagemaker:ListModelQualityJobDefinitions",
            "sagemaker:ListModels",
            "sagemaker:ListMonitoringExecutions",
            "sagemaker:ListMonitoringSchedules",
            "sagemaker:ListNotebookInstanceLifecycleConfigs",
            "sagemaker:ListNotebookInstances",
```

```
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
```

```
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata all' AWS CodeBuild interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a un sottoinsieme di servizi correlati, tra cui CodePipeline, e altri. CodeBuild

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 marzo 2022, 04:27 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRWritePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildPassRoletPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com",
            "codepipeline.amazonaws.com",
            "cloudformation.amazonaws.com",
            "codebuild.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildLogPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
```

```
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
```

```
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
```

```
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
```

```
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
```

```
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
```

```
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
```

```
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
```

```
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

Descrizione: politica relativa al ruolo di servizio utilizzata all' AWS CodePipeline interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a un sottoinsieme di servizi correlati, tra cui CodePipeline, e altri. CodeBuild

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 febbraio 2022, 09:53 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelinePassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
```

```
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata dagli AWS CloudWatch Eventi all'interno dei AWS ServiceCatalog prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a un sottoinsieme di servizi correlati, inclusi altri. CodePipeline

`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 febbraio 2022, 09:53 UTC
- Ora modificata: 22 febbraio 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "codepipeline:StartPipelineExecution",
      "Resource" : "arn:aws:codepipeline:*:*:sagemaker-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata da AWS Firehose nell'ambito dei prodotti AWS ServiceCatalog forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni per una serie di servizi correlati, tra cui Firehose e altri.

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 22 febbraio 2022, 09:54 UTC
- Ora modificata: 22 febbraio 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Descrizione: politica relativa al ruolo di servizio utilizzata da AWS Glue all'interno AWS ServiceCatalog dei prodotti forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni a una serie di servizi correlati tra cui Glue, S3 e altri.

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 febbraio 2022, 09:51 UTC
- Ora modificata: 26 agosto 2022, 19:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchCreatePartition",
```

```
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeletePartition",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetDatabase",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:SearchTables",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:tableVersion/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/glue/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Descrizione: politica del ruolo di servizio utilizzata da AWS Lambda all'interno dei prodotti AWS ServiceCatalog forniti dal SageMaker portafoglio di prodotti Amazon. Concede le autorizzazioni per una serie di servizi correlati tra cui ECR, S3 e altri.

`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 4 aprile 2022, 16:34 UTC
- Ora modificata: 11 giugno 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerLambdaECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
```

```
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
```

```
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
```

```
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
```

```
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
```

```
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
```

```
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
```

```
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:algorithm/*",
        "arn:aws:sagemaker:*:*:app-image-config/*",
        "arn:aws:sagemaker:*:*:artifact/*",
        "arn:aws:sagemaker:*:*:automl-job/*",
        "arn:aws:sagemaker:*:*:code-repository/*",
        "arn:aws:sagemaker:*:*:compilation-job/*",
        "arn:aws:sagemaker:*:*:context/*",
        "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
        "arn:aws:sagemaker:*:*:device-fleet/*",
        "arn:aws:sagemaker:*:*:edge-packaging-job/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:experiment/*",
        "arn:aws:sagemaker:*:*:experiment-trial/*",
```

```
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:feature-group/*",
        "arn:aws:sagemaker:*:*:human-loop/*",
        "arn:aws:sagemaker:*:*:human-task-ui/*",
        "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
        "arn:aws:sagemaker:*:*:image/*",
        "arn:aws:sagemaker:*:*:image-version/*/*",
        "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
        "arn:aws:sagemaker:*:*:labeling-job/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
        "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:monitoring-schedule/*",
        "arn:aws:sagemaker:*:*:notebook-instance/*",
        "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:pipeline/*/execution/*",
        "arn:aws:sagemaker:*:*:processing-job/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:transform-job/*",
        "arn:aws:sagemaker:*:*:workforce/*",
        "arn:aws:sagemaker:*:*:workteam/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaLogPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
```

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    },
    {
      "Sid" : "AmazonSageMakerLambdaCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/sagemaker-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:project-name" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerSpacesControllerPolicy

Descrizione: concede a Systems Manager le autorizzazioni di attivazione, gestione delle sessioni e operazioni chiave KMS necessarie per l'addon SageMaker Spaces per consentire l'accesso remoto sicuro a EKS Spaces. SageMaker

`AmazonSageMakerSpacesControllerPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerSpacesControllerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 novembre 2025, 04:34 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesControllerPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOperatorToSSMCreateActivationForSpaces",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeActivations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeActivations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeSessions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeleteActivation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToActivation",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
```

```
        "arn:aws:iam::*:role/sagemaker-space-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeManagedNodes",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeregisterWorkspaceInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToPassSsmManagedNodeRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/sagemaker-space-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowOperatorToSSMStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowStartSessionDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-StartSSHSession",
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "AllowOperatorToSSMCreateDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToEnableAdvancedTierForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting",
        "ssm:ResetServiceSetting"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/activation-
tier"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToSSMDocument",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerSpacesRouterPolicy

Descrizione: concede a Systems KMS le autorizzazioni operative chiave necessarie affinché il router SageMaker Spaces consenta l'accesso remoto sicuro a EKS Spaces. SageMaker

`AmazonSageMakerSpacesRouterPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerSpacesRouterPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 19 novembre 2025, 04:34 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesRouterPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSageMakerTrainingPlanCreateAccess

Descrizione: questa Amazon Managed Policy fornisce le autorizzazioni necessarie per creare e gestire i piani di SageMaker formazione. Consente agli utenti di creare piani di formazione e capacità riservate, descrivere piani di formazione esistenti ed eseguire operazioni di ricerca ed elenco.

`AmazonSageMakerTrainingPlanCreateAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSageMakerTrainingPlanCreateAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 dicembre 2024, 13:21 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerTrainingPlanCreateAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingPlan",
        "sagemaker:CreateReservedCapacity",
        "sagemaker:DescribeReservedCapacity"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AddTagsToTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateTrainingPlan",
            "CreateReservedCapacity"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeTrainingPlan",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*"
```

```
      ]
    },
    {
      "Sid" : "NonResourceLevelTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SearchTrainingPlanOfferings",
        "sagemaker:ListTrainingPlans"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListUltraServersByReservedCapacityPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListUltraServersByReservedCapacity",
      "Resource" : [
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSecurityLakeAdministrator

Descrizione: fornisce l'accesso completo ad Amazon Security Lake e ai servizi correlati necessari per amministrare Security Lake.

`AmazonSecurityLakeAdministrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSecurityLakeAdministrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 maggio 2023, 22:04 UTC
- Ora modificata: 23 febbraio 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:StopCrawlerSchedule",
        "lambda:CreateEventSourceMapping",
```

```
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDatalakeSettings",
        "events:ListConnections",
        "events:ListApiDestinations",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagingSecurityLakeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaCreateFunction",
```

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaAddPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringEquals" : {
          "lambda:Principal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "glue:CreateTable",
        "glue:GetTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
```

```
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule",
        "events:CreateApiDestination",
        "events:CreateConnection",
        "events:UpdateConnection",
        "events:UpdateApiDestination",
        "events:DeleteConnection",
        "events:DeleteApiDestination",
        "events:ListTargetsByRule",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonSecurityLake*",
        "arn:aws:events:*:*:rule/SecurityLake*",
        "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
        "arn:aws:events:*:*:connection/AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSQSActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
```

```
        "sqs:GetQueueURL",
        "sqs:AddPermission",
        "sqs:GetQueueAttributes",
        "sqs:DeleteQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake*",
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsCmkGrantForSecurityLake",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "GenerateDataKey",
            "RetireGrant",
            "Decrypt"
          ]
        }
      }
    },
    {
      "Sid" : "AllowEnablingQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:ResourceArn" : [
            "arn:aws:glue:*:*:catalog",
            "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
            "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfiguringQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:GetResourceShares",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "LakeFormation*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
            "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "StringLike" : {
```

```
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:subscriber/*"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
```

```
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:events:*:*:rule/AmazonSecurityLake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOnboardingToSecurityLakeDependencies",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
        "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
        "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "securitylake.amazonaws.com",
            "lakeformation.amazonaws.com",
            "apidestinations.events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowRolePolicyActionsforSubscibersandSources",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowRegisterS3LocationInLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PutRolePolicy",
        "iam:GetRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowIAMActionsByResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRolePolicies",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakes",
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake-*"
    },
    {
```

```
      "Sid" : "S3ReadAccessToSecurityLakeMetastoreObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::security-lake-meta-store-manager-*"
    },
    {
      "Sid" : "S3ResourcelessReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSecurityLakeMetastoreManager

Descrizione: Policy per Amazon SecurityLake meta store manager lambda che consente l'accesso a cloudwatch, S3, Glue e SQS.

`AmazonSecurityLakeMetastoreManager`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSecurityLakeMetastoreManager` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 23 gennaio 2024, 15:26 UTC
- Ora modificata: 01 aprile 2024, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowGlueManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToReadFromSqs",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataReadWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCleanup",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSecurityLakePermissionsBoundary

Descrizione: Amazon Security Lake crea ruoli IAM per fonti personalizzate di terze parti per scrivere dati su un data lake e per gli abbonati di terze parti per utilizzare i dati da un data lake e utilizza questa politica durante la creazione di questi ruoli per definire i limiti delle loro autorizzazioni.

`AmazonSecurityLakePermissionsBoundary`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonSecurityLakePermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2022, 14:11 UTC
- Ora modificata: 14 maggio 2024, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsForSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
```

```
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyActionsForSecurityLake",
      "Effect" : "Deny",
      "NotAction" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeBucket",
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource" : [
        "arn:aws:s3:::aws-security-data-lake*"
```

```
      ]
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeSQS",
      "Effect" : "Deny",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
```

```
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sqs:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:sqs:arn" : [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSESFullAccess

Descrizione: fornisce l'accesso completo ad Amazon SES tramite Console di gestione AWS.

`AmazonSESFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSESFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSESReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon SES tramite Console di gestione AWS.

`AmazonSESReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSESReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 14 maggio 2024, 12:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SESReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ses:Get*",
        "ses:List*",
        "ses:BatchGetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSESServiceRolePolicy

Descrizione: consente a SES di pubblicare i parametri CloudWatch di monitoraggio di Amazon Basic per conto delle tue risorse SES

`AmazonSESServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 maggio 2024, 16:02 UTC
- Ora modificata: 21 maggio 2024, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricDataToSESCloudWatchNamespaces",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "AWS/SES",
            "AWS/SES/MailManager",
            "AWS/SES/Addons"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSNSFullAccess

Descrizione: fornisce l'accesso completo ad Amazon SNS tramite. Console di gestione AWS

`AmazonSNSFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSNSFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 24 settembre 2024, 22:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSFullAccess",
      "Effect" : "Allow",
      "Action" : "sns:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:CreateVerifiedDestinationNumber",
        "sms-voice:SendDestinationNumberVerificationCode",
        "sms-voice:SendTextMessage",
        "sms-voice:DeleteVerifiedDestinationNumber",
        "sms-voice:VerifyDestinationNumber",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:SetTextMessageSpendLimitOverride",
```

```
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DeleteOptedOutNumber"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSNSReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon SNS tramite. Console di gestione AWS

`AmazonSNSReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSNSReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 24 settembre 2024, 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:List*",
        "sns:CheckIfPhoneNumberIsOptedOut",
        "sns:GetEndpointAttributes",
        "sns:GetDataProtectionPolicy",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetSMSAttributes",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribeOptedOutNumbers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSNSRole

Descrizione: policy predefinita per il ruolo del servizio Amazon SNS.

`AmazonSNSRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSNSRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSQSFullAccess

Descrizione: fornisce l'accesso completo ad Amazon SQS tramite. Console di gestione AWS

`AmazonSQSFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSQSFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sqs:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSQSReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon SQS tramite. Console di gestione AWS

`AmazonSQSReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSQSReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 24 maggio 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSSMAutomationApproverAccess

Descrizione: fornisce l'accesso per visualizzare le esecuzioni di automazione e inviare le decisioni di approvazione all'automazione in attesa di approvazione

`AmazonSSMAutomationApproverAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSSMAutomationApproverAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 agosto 2017, 23:07 UTC
- Ora modificata: 07 agosto 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution",
        "ssm:SendAutomationSignal"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSSMAutomationRole

Descrizione: fornisce le autorizzazioni al servizio EC2 Automation per eseguire le attività definite nei documenti di automazione

`AmazonSSMAutomationRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSSMAutomationRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 dicembre 2016, 22:09 UTC
- Ora modificata: 20 marzo 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DeleteSnapshot",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
```

```
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:session/*"
      ]
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSSMDirectoryServiceAccess

Descrizione: questo criterio consente all'agente SSM di accedere al Directory Service per conto del cliente per l'aggiunta al dominio dell'istanza gestita.

`AmazonSSMDirectoryServiceAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonSSMDirectoryServiceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 marzo 2019, 17:44 UTC
- Ora modificata: 15 marzo 2019, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSSMFullAccess

Descrizione: fornisce l'accesso completo ad Amazon SSM.

`AmazonSSMFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSSMFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 maggio 2015, 17:39 UTC
- Ora modificata: 20 novembre 2019, 20:08 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeInstanceStatus",
        "logs:*",
        "ssm:*",
        "ec2messages:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSSMMaintenanceWindowRole

Descrizione: ruolo di servizio da utilizzare per la finestra di manutenzione di EC2

`AmazonSSMMaintenanceWindowRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSSMMaintenanceWindowRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2016, 15:57 UTC

- Ora modificata: 27 luglio 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSSMManagedEC2InstanceDefaultPolicy

Descrizione: questa policy abilita la funzionalità AWS Systems Manager sulle istanze EC2.

`AmazonSSMManagedEC2InstanceDefaultPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSSMManagedEC2InstanceDefaultPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 agosto 2022, 20:54 UTC
- Ora modificata: 16 luglio 2024, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMAgentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
```

```
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSMChannelMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSMLegacyMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSSMManagedInstanceCore

Descrizione: la policy per il ruolo di Amazon EC2 per abilitare le funzionalità principali del servizio AWS Systems Manager.

`AmazonSSMManagedInstanceCore`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSSMManagedInstanceCore` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 marzo 2019, 17:22 UTC
- Ora modificata: 23 maggio 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
```

```
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSSMPatchAssociation

Descrizione: fornisce l'accesso alle istanze secondarie per le operazioni di associazione delle patch.

`AmazonSSMPatchAssociation`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSSMPatchAssociation` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 maggio 2020, 16:00 UTC
- Ora modificata: 13 maggio 2020, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribeEffectivePatchesForPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "ssm:GetPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribePatchBaselines",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSSMReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon SSM.

`AmazonSSMReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSSMReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 maggio 2015, 17:44 UTC
- Ora modificata: 29 maggio 2015, 17:44 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSSMServiceRolePolicy

Descrizione: Fornisce l'accesso alle AWS risorse gestite o utilizzate da Amazon SSM

`AmazonSSMServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 13 novembre 2017, 19:20 UTC
- Ora modificata: 26 giugno 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Versione della politica

Versione della politica: v17 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState",
        "ssm:ListCloudConnectors"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutInventory"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "ssm:InventoryTypeName" : [
            "AWS:ComplianceItem",
            "AWS:PatchSummary"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:SelectResourceConfig"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEnrollmentStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeCases"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeComplianceByResource",
        "config:DescribeRemediationConfigurations",
```

```
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStackSets",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackInstances",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "cloudformation:DeleteStackInstances",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SSMExplorerManagedRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:DescribeRule",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "securityhub:DescribeHub",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-explorer-2:CreateManagedView",
      "Resource" : "arn:aws:resource-explorer-2:*:*:managed-view/AWSManagedViewForSSM*"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonSumerianFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Sumerian.

`AmazonSumerianFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonSumerianFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 aprile 2018, 20:14 UTC
- Ora modificata: 24 aprile 2018, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sumerian:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonTextractFullAccess

Descrizione: Accesso a tutti gli Amazon Textract APIs

`AmazonTextractFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonTextractFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 19:07 UTC
- Ora modificata: 28 novembre 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonTextractServiceRole

Descrizione: consente a Textract di chiamare AWS i servizi per tuo conto.

`AmazonTextractServiceRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonTextractServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 28 novembre 2018, 19:12 UTC
- Ora modificata: 28 novembre 2018, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonTextract*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonTimestreamConsoleFullAccess

Descrizione: fornisce l'accesso completo alla gestione di Amazon Timestream utilizzando. Console di gestione AWS Tieni presente che questa politica concede anche le autorizzazioni per determinate

operazioni KMS e operazioni per la gestione delle query salvate. Se utilizzi la CMK gestita dal cliente, consulta la documentazione per le autorizzazioni aggiuntive necessarie.

`AmazonTimestreamConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonTimestreamConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 settembre 2020, 21:47 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
```

```
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:ListEntitlementDetails",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:Subscribe"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-5jijo74ujy36m",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonTimestreamFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Timestream. Tieni presente che questa politica concede anche determinati accessi operativi KMS. Se utilizzi la CMK gestita dal cliente, consulta la documentazione per le autorizzazioni aggiuntive necessarie.

`AmazonTimestreamFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonTimestreamFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 settembre 2020, 21:47 UTC
- Ora modificata: 26 novembre 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonTimestreamInfluxDBFullAccess

Descrizione: fornisce l'accesso amministrativo completo per creare, aggiornare, eliminare ed elencare le istanze Amazon Timestream InfluxDB e creare ed elencare gruppi di parametri. Fai riferimento alla documentazione per le autorizzazioni aggiuntive necessarie.

`AmazonTimestreamInfluxDBFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonTimestreamInfluxDBFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 marzo 2024, 22:53 UTC
- Ora modificata: 3 agosto 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Versione della politica

Versione della politica: v18 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster",
        "timestream-influxdb:CreateDbBackup",
        "timestream-influxdb:GetDbBackup",
        "timestream-influxdb:ListDbBackups",
        "timestream-influxdb:DeleteDbBackup",
        "timestream-influxdb:RestoreFromDbBackup"
      ],
      "Resource" : "arn:aws:timestream-influxdb:*:*:*"
```

```
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid" : "MPViewAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MPSubscriptionAccessStatement",
      "Effect" : "Allow",
      "Action" : "aws-marketplace:Subscribe",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess

Descrizione: fornisce l'accesso amministrativo per gestire le istanze InfluxDB e i gruppi di parametri di Amazon Timestream, ad eccezione delle operazioni sul marketplace.

`AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 aprile 2025, 17:52 UTC
- Ora modificata: 3 agosto 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`

Versione della politica

Versione della politica: v10 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
```

```
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster",
        "timestream-influxdb:CreateDbBackup",
        "timestream-influxdb:GetDbBackup",
        "timestream-influxdb:ListDbBackups",
        "timestream-influxdb:DeleteDbBackup",
        "timestream-influxdb:RestoreFromDbBackup"
      ],
      "Resource" : [
        "arn:aws:timestream-influxdb:*:*:*"
      ]
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonTimestreamInfluxDBServiceRolePolicy

Descrizione: fornisce l'accesso amministrativo completo per creare, aggiornare, eliminare ed elencare le istanze Amazon Timestream InfluxDB e creare ed elencare gruppi di parametri. Fai riferimento alla documentazione per le autorizzazioni aggiuntive necessarie.

`AmazonTimestreamInfluxDBServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 14 marzo 2024, 18:53 UTC
- Ora modificata: 20 luglio 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Versione della politica

Versione della politica: v2 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "CreateEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateTagWithEniStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PutCloudWatchMetricsStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Timestream/InfluxDB",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:READONLY-InfluxDB-auth-parameters-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RetrievePluginSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:InfluxDB-RepoToken-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DecryptPluginSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:*:kms:*:${aws:PrincipalAccount}:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" :
 "arn:*:secretsmanager:*:*:secret:InfluxDB-RepoToken-*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonTimestreamReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Timestream. La policy fornisce inoltre l'autorizzazione per annullare qualsiasi query in esecuzione. Se utilizzi la CMK gestita dal cliente, consulta la documentazione per le autorizzazioni aggiuntive necessarie.

`AmazonTimestreamReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonTimestreamReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 settembre 2020, 21:47 UTC
- Ora modificata: 5 giugno 2024, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonTimestreamReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:CancelQuery",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:Select",
        "timestream:SelectValues",
        "timestream:DescribeScheduledQuery",
        "timestream:ListScheduledQueries",
        "timestream:DescribeBatchLoadTask",
        "timestream:ListBatchLoadTasks",
        "timestream:DescribeAccountSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonTranscribeFullAccess

Descrizione: Fornisce accesso completo alle operazioni di Amazon Transcribe

`AmazonTranscribeFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonTranscribeFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 aprile 2018, 16:06 UTC
- Ora modificata: 4 aprile 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonTranscribeReadOnlyAccess

Descrizione: fornisce l'accesso alle operazioni di sola lettura per Amazon Transcribe

`AmazonTranscribeReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonTranscribeReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 aprile 2018, 16:05 UTC
- Ora modificata: 4 aprile 2018, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:Get*",
        "transcribe:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonVerifiedPermissionsFullAccess

Descrizione: fornisce l'accesso completo alle autorizzazioni verificate

`AmazonVerifiedPermissionsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonVerifiedPermissionsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 ottobre 2024, 18:19 UTC
- Ora modificata: 11 ottobre 2024, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:CreatePolicyStore",
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:*"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonVerifiedPermissionsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura al servizio Autorizzazioni verificate.

`AmazonVerifiedPermissionsReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonVerifiedPermissionsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 ottobre 2024, 18:25 UTC
- Ora modificata: 11 ottobre 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyTemplates"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonVPCCrossAccountNetworkInterfaceOperations

Descrizione: fornisce l'accesso per creare interfacce di rete e collegarle a risorse tra account diversi

`AmazonVPCCrossAccountNetworkInterfaceOperations`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonVPCCrossAccountNetworkInterfaceOperations` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 luglio 2017, 20:47 UTC
- Ora modificata: 25 settembre 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:ReplaceRoute"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonVPCFullAccess

Descrizione: fornisce l'accesso completo ad Amazon VPC tramite. Console di gestione AWS

`AmazonVPCFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonVPCFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSecurityGroupVpc",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
```

```
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpcPeeringConnection",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
```

```
            "ec2:DescribeInstances",
            "ec2:DescribeInternetGateways",
            "ec2:DescribeIpv6Pools",
            "ec2:DescribeLocalGatewayRouteTables",
            "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
            "ec2:DescribeKeyPairs",
            "ec2:DescribeMovingAddresses",
            "ec2:DescribeNatGateways",
            "ec2:DescribeNetworkAcls",
            "ec2:DescribeNetworkInterfaceAttribute",
            "ec2:DescribeNetworkInterfacePermissions",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribePrefixLists",
            "ec2:DescribeRouteTables",
            "ec2:DescribeSecurityGroupReferences",
            "ec2:DescribeSecurityGroupRules",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSecurityGroupVpcAssociations",
            "ec2:DescribeStaleSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeTags",
            "ec2:DescribeVpcAttribute",
            "ec2:DescribeVpcClassicLink",
            "ec2:DescribeVpcClassicLinkDnsSupport",
            "ec2:DescribeVpcEndpointConnectionNotifications",
            "ec2:DescribeVpcEndpointConnections",
            "ec2:DescribeVpcEndpoints",
            "ec2:DescribeVpcEndpointServiceConfigurations",
            "ec2:DescribeVpcEndpointServicePermissions",
            "ec2:DescribeVpcEndpointServices",
            "ec2:DescribeVpcPeeringConnections",
            "ec2:DescribeVpcs",
            "ec2:DescribeVpnConnections",
            "ec2:DescribeVpnGateways",
            "ec2:DetachClassicLinkVpc",
            "ec2:DetachInternetGateway",
            "ec2:DetachNetworkInterface",
            "ec2:DetachVpnGateway",
            "ec2:DisableVgwRoutePropagation",
            "ec2:DisableVpcClassicLink",
            "ec2:DisableVpcClassicLinkDnsSupport",
            "ec2:DisassociateAddress",
            "ec2:DisassociateRouteTable",
            "ec2:DisassociateSecurityGroupVpc",
```

```
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLink",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:RejectVpcPeeringConnection",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

Descrizione: fornisce le autorizzazioni per descrivere AWS le risorse, eseguire Network Access Analyzer e creare o eliminare tag su Network Insights Access Scope e Network Insights Access Scope Analysis.

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 giugno 2023, 22:56 UTC
- Ora modificata: 15 maggio 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScopeAnalysis",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAccessScopeAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-access-scope/*",
        "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
```

```
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TirosPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonVPCReachabilityAnalyzerFullAccessPolicy

Descrizione: fornisce le autorizzazioni per descrivere AWS le risorse, eseguire Reachability Analyzer e creare o eliminare tag su Network Insights Path e Network Insights Analysis.

`AmazonVPCReachabilityAnalyzerFullAccessPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonVPCReachabilityAnalyzerFullAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 giugno 2023, 20:12 UTC
- Ora modificata: 15 maggio 2024, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-path/*",
        "arn:*:ec2:*:*:network-insights-analysis/*"
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TirosPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Descrizione: questa politica è allegata al ruolo IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess. Questo ruolo viene distribuito agli account dei membri di un'organizzazione quando l'account di gestione consente l'accesso affidabile per Reachability Analyzer. Fornisce le autorizzazioni per visualizzare le risorse di tutta l'organizzazione utilizzando la console Reachability Analyzer.

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 maggio 2023, 20:38 UTC
- Ora modificata: 01 maggio 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonVPCReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon VPC tramite. Console di gestione AWS

`AmazonVPCReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonVPCReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkDocsFullAccess

Descrizione: Fornisce l'accesso completo ad Amazon WorkDocs tramite Console di gestione AWS

`AmazonWorkDocsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkDocsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 aprile 2020, 23:05 UTC
- Ora modificata: 16 aprile 2020, 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkDocsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon WorkDocs tramite Console di gestione AWS

`AmazonWorkDocsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkDocsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 gennaio 2020, 23:49 UTC
- Ora modificata: 08 gennaio 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkMailEventsServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Amazon WorkMail Events

`AmazonWorkMailEventsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 16 aprile 2019, 16:52 UTC
- Ora modificata: 16 aprile 2019, 16:52 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkMailFullAccess

Descrizione: Fornisce accesso completo ai metadati KMS WorkMail, Directory Service, SES, EC2 e accesso in lettura ai metadati KMS.

`AmazonWorkMailFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkMailFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 21 dicembre 2020, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
```

```
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "events.workmail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.workmail.amazonaws.com/
AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*workmail*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.workmail.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkMailMessageFlowFullAccess

Descrizione: accesso completo al flusso di WorkMail messaggi APIs

`AmazonWorkMailMessageFlowFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkMailMessageFlowFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 11 febbraio 2021, 11:08 UTC
- Ora modificata: 11 febbraio 2021, 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workmailmessageflow:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkMailMessageFlowReadOnlyAccess

Descrizione: accesso in sola lettura ai WorkMail messaggi per l' GetRawMessageContent API

`AmazonWorkMailMessageFlowReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkMailMessageFlowReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 gennaio 2021, 12:40 UTC
- Ora modificata: 28 gennaio 2021, 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workmailmessageflow:Get*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkMailReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a WorkMail e SES.

`AmazonWorkMailReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkMailReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 25 luglio 2019, 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesAdmin

Descrizione: fornisce l'accesso alle azioni WorkSpaces amministrative di Amazon tramite AWS SDK e CLI.

`AmazonWorkSpacesAdmin`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkSpacesAdmin` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 settembre 2015, 22:21 UTC

- Ora modificata: 27 giugno 2024, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonWorkSpacesAdmin",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateWorkspacesPool",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces:DeleteTags",
        "workspaces:DeregisterWorkspaceDirectory",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesPools",
        "workspaces:DescribeWorkspacesPoolSessions",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyStreamingProperties",
        "workspaces:ModifyWorkspaceCreationProperties",
        "workspaces:ModifyWorkspaceProperties",
```

```
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:RegisterWorkspaceDirectory",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
        "workspaces:StartWorkspacesPool",
        "workspaces:StopWorkspaces",
        "workspaces:StopWorkspacesPool",
        "workspaces:TerminateWorkspaces",
        "workspaces:TerminateWorkspacesPool",
        "workspaces:TerminateWorkspacesPoolSession",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesApplicationManagerAdminAccess

Descrizione: fornisce l'accesso di amministratore per il pacchetto di un'applicazione in Amazon WorkSpaces Application Manager.

`AmazonWorkSpacesApplicationManagerAdminAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkSpacesApplicationManagerAdminAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 9 aprile 2015, 14:03 UTC
- Ora modificata: 9 aprile 2015, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wam:AuthenticatePackager",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkspacesPCAAccess

Descrizione: questa policy gestita fornisce l'accesso amministrativo completo alle risorse CA private di AWS Certificate Manager Account AWS per l'autenticazione basata su certificati.

`AmazonWorkspacesPCAAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkspacesPCAAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 08 novembre 2022, 00:25 UTC
- Ora modificata: 08 novembre 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesPoolServiceAccess

Descrizione: questa politica fornisce l'accesso al AWS WorkSpaces servizio alle risorse dell'account cliente necessarie per l'avvio di Workspaces Pools

`AmazonWorkSpacesPoolServiceAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkSpacesPoolServiceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2024, 16:21 UTC
- Ora modificata: 27 giugno 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesPoolServiceAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProvisioningWorkSpacesPoolPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "WorkSpacesPoolS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::wspool-logs-*",
        "arn:aws:s3:::wspool-app-settings-*",
        "arn:aws:s3:::wspool-home-folder-*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesSecureBrowserReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon WorkSpaces Secure Browser e alle sue dipendenze tramite SDK e Console di gestione AWS CLI.

`AmazonWorkSpacesSecureBrowserReadOnly`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkSpacesSecureBrowserReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2024, 20:01 UTC
- Ora modificata: 24 giugno 2024, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSecureBrowserReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesSecureBrowser",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetIpAccessSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListIpAccessSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Sid" : "Dependencies",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesSelfServiceAccess

Descrizione: Fornisce l'accesso al servizio di WorkSpaces backend Amazon per eseguire azioni self-service di Workspace

`AmazonWorkSpacesSelfServiceAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkSpacesSelfServiceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2019, 19:22 UTC
- Ora modificata: 27 giugno 2019, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesServiceAccess

Descrizione: fornisce all'account del cliente l'accesso al AWS WorkSpaces servizio per l'avvio di un Workspace.

`AmazonWorkSpacesServiceAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkSpacesServiceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2019, 19:19 UTC
- Ora modificata: 18 marzo 2020, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesThinClientFullAccess

Descrizione: Fornisce accesso completo ad Amazon WorkSpaces Thin Client e accesso limitato ai servizi correlati richiesti

`AmazonWorkSpacesThinClientFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkSpacesThinClientFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 agosto 2024, 07:25 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
monitoring.thinclient.amazonaws.com/
AWSServiceRoleForAmazonWorkSpacesThinClientMonitoring",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitoring.thinclient.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Amazon WorkSpaces Thin Client Monitoring

`AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 13 giugno 2025, 19:37 UTC
- Ora modificata: 13 giugno 2025, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/WorkSpacesThinClient",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesThinClientReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon WorkSpaces Thin Client e alle sue dipendenze

`AmazonWorkSpacesThinClientReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkSpacesThinClientReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 luglio 2024, 08:50 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesWebReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon WorkSpaces Web e alle sue dipendenze tramite SDK e Console di gestione AWS CLI.

`AmazonWorkSpacesWebReadOnly`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmazonWorkSpacesWebReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2021, 14:20 UTC
- Ora modificata: 02 novembre 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
```

```
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonWorkSpacesWebServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Amazon WorkSpaces Web

`AmazonWorkSpacesWebServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 30 novembre 2021, 13:15 UTC
- Ora modificata: 15 dicembre 2022, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/WorkSpacesWebManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "WorkSpacesWebManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/WorkSpacesWebManaged" : "true"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/WorkSpacesWeb",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStreamSummary"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonZocaloFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Zocalo.

`AmazonZocaloFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonZocaloFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:*",
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmazonZocaloReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ad Amazon Zocalo

`AmazonZocaloReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AmazonZocaloReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AmplifyBackendDeployFullAccess

Descrizione: Fornisce le autorizzazioni di accesso completo ad Amplify per distribuire le risorse di backend Amplify (AWS AppSyncAmazon Cognito, Amazon S3 e altri servizi correlati) tramite il Development Kit (CDK) Cloud AWS AWS

`AmplifyBackendDeployFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AmplifyBackendDeployFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 ottobre 2023, 21:32 UTC
- Ora modificata: 14 novembre 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetSchemaCreationStatus",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:ListFunctions",
        "appsync:UpdateFunction",
        "appsync:UpdateApiKey"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableFunctionResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
```

```
        "arn:aws:lambda:*:*:function:amplify-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingListTags",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListTags"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ]
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/amplify-*:*",
        "arn:aws:logs:*:*:log-group:amplify-*:*"
      ]
    },
    {
      "Sid" : "AmplifySchema",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*amplify*",
        "arn:aws:s3:::cdk-*-assets-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "CDKDeploy",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
        "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amplify/*",
        "arn:aws:ssm:*:*:parameter/cdk-bootstrap/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyModifySSMParam",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:DeleteParameters"
```

```
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyDiscoverRDSVpcConfig",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBProxies",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "ec2:DescribeSubnets",
        "rds:DescribeDBSubnetGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db-proxy:*",
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AnthropicFullAccess

Descrizione: Fornisce l'accesso completo alla piattaforma Claude su AWS

`AnthropicFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AnthropicFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2026, 04:57 UTC
- Ora modificata: 01 aprile 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicSubscriptionManagement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-3qbeiztufnva6"
          ]
        }
      }
    },
    {
      "Sid" : "AnthropicSubscriptionView",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicFullEnableFederation",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetOutboundWebIdentityFederationInfo",
        "iam:EnableOutboundWebIdentityFederation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicFullGetToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "sts:IdentityTokenAudience" : [
            "https://api.anthropic.com",
            "https://platform.claude.com"
          ]
        },
        "StringEquals" : {
```

```
          "aws:CalledViaLast" : "aws-external-anthropic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnthropicFullTagToken",
      "Effect" : "Allow",
      "Action" : "sts:TagGetWebIdentityToken",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AnthropicInferenceAccess

Descrizione: Fornisce accesso in lettura e inferenza alla piattaforma Claude su AWS

`AnthropicInferenceAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AnthropicInferenceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2026, 04:57 UTC
- Ora modificata: 01 aprile 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicInferenceAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicInferenceWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:Get*",
        "aws-external-anthropic:List*",
        "aws-external-anthropic:CreateInference",
        "aws-external-anthropic:CreateBatchInference",
        "aws-external-anthropic:CancelBatchInference",
        "aws-external-anthropic:DeleteBatchInference",
        "aws-external-anthropic:CountTokens"
      ],
      "Resource" : "arn:aws:aws-external-anthropic:*:*:workspace/*"
    },
    {
      "Sid" : "AnthropicInferenceResourceless",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:GetAccountStatus",
        "aws-external-anthropic:CallWithBearerToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicInferenceGetToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "sts:IdentityTokenAudience" : [
            "https://api.anthropic.com",
            "https://platform.claude.com"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : "aws-external-anthropic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnthropicInferenceTagToken",
      "Effect" : "Allow",
      "Action" : "sts:TagGetWebIdentityToken",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AnthropicLimitedAccess

Descrizione: Fornisce un accesso limitato alla piattaforma Claude su AWS

`AnthropicLimitedAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AnthropicLimitedAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2026, 04:57 UTC

- Ora modificata: 12 giugno 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicLimitedAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicLimitedWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:Get*",
        "aws-external-anthropic:List*",
        "aws-external-anthropic:ArchiveAgent",
        "aws-external-anthropic:ArchiveEnvironment",
        "aws-external-anthropic:ArchiveMemoryStore",
        "aws-external-anthropic:ArchiveSession",
        "aws-external-anthropic:ArchiveVault",
        "aws-external-anthropic:CancelBatchInference",
        "aws-external-anthropic:CountTokens",
        "aws-external-anthropic:CreateAgent",
        "aws-external-anthropic:CreateBatchInference",
        "aws-external-anthropic:CreateEnvironment",
        "aws-external-anthropic:CreateFile",
        "aws-external-anthropic:CreateInference",
        "aws-external-anthropic:CreateMemoryStore",
        "aws-external-anthropic:CreateSession",
        "aws-external-anthropic:CreateSkill",
        "aws-external-anthropic:CreateUserProfile",
        "aws-external-anthropic:CreateVault",
        "aws-external-anthropic:CreateWebhook",
        "aws-external-anthropic:DeleteBatchInference",
        "aws-external-anthropic:DeleteEnvironment",
```

```
        "aws-external-anthropic:DeleteFile",
        "aws-external-anthropic:DeleteMemoryStore",
        "aws-external-anthropic:DeleteSession",
        "aws-external-anthropic:DeleteSkill",
        "aws-external-anthropic:DeleteVault",
        "aws-external-anthropic:DeleteWebhook",
        "aws-external-anthropic:ProcessEnvironmentWork",
        "aws-external-anthropic:RotateWebhookSecret",
        "aws-external-anthropic:UpdateAgent",
        "aws-external-anthropic:UpdateEnvironment",
        "aws-external-anthropic:UpdateMemoryStore",
        "aws-external-anthropic:UpdateSession",
        "aws-external-anthropic:UpdateSkill",
        "aws-external-anthropic:UpdateUserProfile",
        "aws-external-anthropic:UpdateVault",
        "aws-external-anthropic:UpdateWebhook"
      ],
      "Resource" : "arn:aws:aws-external-anthropic:*:*:workspace/*"
    },
    {
      "Sid" : "AnthropicLimitedResourceless",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:GetAccountStatus",
        "aws-external-anthropic:CallWithBearerToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicLimitedGetToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "sts:IdentityTokenAudience" : [
            "https://api.anthropic.com",
            "https://platform.claude.com"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : "aws-external-anthropic.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AnthropicLimitedTagToken",
      "Effect" : "Allow",
      "Action" : "sts:TagGetWebIdentityToken",
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicLimitedConsoleAccess",
      "Effect" : "Allow",
      "Action" : "aws-external-anthropic:AssumeConsole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-external-anthropic:Capability" : "developer"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AnthropicReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alla piattaforma Claude su AWS

`AnthropicReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AnthropicReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2026, 04:57 UTC
- Ora modificata: 01 aprile 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicReadOnlyWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:Get*",
        "aws-external-anthropic:List*"
      ],
      "Resource" : "arn:aws:aws-external-anthropic:*:*:workspace/*"
    },
    {
      "Sid" : "AnthropicReadOnlyResourceless",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:GetAccountStatus",
        "aws-external-anthropic:CallWithBearerToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicReadOnlyGetToken",
```

```
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "sts:IdentityTokenAudience" : [
            "https://api.anthropic.com",
            "https://platform.claude.com"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : "aws-external-anthropic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnthropicReadOnlyTagToken",
      "Effect" : "Allow",
      "Action" : "sts:TagGetWebIdentityToken",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AnthropicSelfHostedEnvironmentAccess

Descrizione: Fornisce l'accesso alla gestione di un ambiente di esecuzione ospitato autonomamente per Claude Managed Agents

`AnthropicSelfHostedEnvironmentAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AnthropicSelfHostedEnvironmentAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 giugno 2026, 17:12 UTC
- Ora modificata: 12 giugno 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicSelfHostedEnvironmentAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicSelfHostedEnvironmentWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:GetEnvironment",
        "aws-external-anthropic:GetSession",
        "aws-external-anthropic:GetSkill",
        "aws-external-anthropic:ProcessEnvironmentWork",
        "aws-external-anthropic:UpdateSession"
      ],
      "Resource" : "arn:aws:aws-external-anthropic:*:*:workspace/*"
    },
    {
      "Sid" : "AnthropicSelfHostedEnvironmentResourceless",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:CallWithBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

APIGatewayServiceRolePolicy

Descrizione: consente ad API Gateway di gestire AWS le risorse associate per conto del cliente.

`APIGatewayServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 ottobre 2017, 17:23 UTC
- Ora modificata: 12 luglio 2021, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/amazon-apigateway-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "acm:DescribeCertificate",
        "acm:GetCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Owner",
            "VpcLinkId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetNamespace",
      "Resource" : "arn:aws:servicediscovery:*:*:namespace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetService",
      "Resource" : "arn:aws:servicediscovery:*:*:service/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AppIntegrationsServiceLinkedRolePolicy

Descrizione: consente di AppIntegrations gestire AppFlow le risorse e pubblicare i dati CloudWatch metrici per tuo conto.

`AppIntegrationsServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 30 settembre 2022, 19:42 UTC
- Ora modificata: 30 settembre 2022, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppIntegrations"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorEntity",
        "appflow:ListConnectorEntities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorProfiles",
        "appflow:UseConnectorProfile"
      ],
      "Resource" : "arn:aws:appflow:*:*:connector-profile/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AppIntegrationsManaged" : "true"
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:TagResource"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppIntegrationsManaged"
          ]
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ApplicationAutoScalingForAmazonAppStreamAccess

Descrizione: politica per abilitare l'autoscaling delle applicazioni per Amazon AppStream

`ApplicationAutoScalingForAmazonAppStreamAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `ApplicationAutoScalingForAmazonAppStreamAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2017, 21:39 UTC
- Ora modificata: 6 febbraio 2017, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite dalla funzionalità di esportazione continua di Application Discovery Service

`ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 09 agosto 2018, 20:22 UTC
- Ora modificata: 13 agosto 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "firehose:DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
    },
    {
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*"
    },
    {
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*/*"
    },
    {
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AppRunnerNetworkingServiceRolePolicy

Descrizione: consente alla AWS AppRunner rete di gestire AWS le risorse correlate per tuo conto.

`AppRunnerNetworkingServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 gennaio 2022, 21:02 UTC
- Ora modificata: 12 gennaio 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSAppRunnerManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "StringLike" : {
          "aws:RequestTag/AWSAppRunnerManaged" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSAppRunnerManaged" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AppRunnerServiceRolePolicy

Descrizione: consente di AWS AppRunner gestire AWS le risorse correlate per tuo conto.

`AppRunnerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 maggio 2021, 19:15 UTC
- Ora modificata: 14 maggio 2021, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apprunner/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apprunner/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSAppRunnerManagedRule*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AppStudioServiceRolePolicy

Descrizione: consente di AppStudio gestire AWS le risorse associate per tuo conto.

`AppStudioServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 luglio 2024, 05:01 UTC
- Ora modificata: 13 marzo 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppStudioServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AppStudioResourcePermissionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appstudio/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "IsAppStudioSecret"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/IsAppStudioSecret" : "true"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForManagedSecrets",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appstudio"
        }
      }
    },
    {
      "Sid" : "AppStudioResourceWritePermissionsForManagedSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso-directory:DescribeUsers",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AuroraDsqlServiceLinkedRolePolicy

Descrizione: Policy per il ruolo collegato al servizio SQL di Amazon Aurora

`AuroraDsqlServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 3 dicembre 2024, 15:06 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AuroraDsqlServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AuroraDSQL",
            "AWS/Usage"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AutoScalingConsoleFullAccess

Descrizione: Fornisce l'accesso completo a Auto Scaling tramite. Console di gestione AWS

`AutoScalingConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AutoScalingConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2017, 19:43 UTC

- Ora modificata: 6 febbraio 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:ImportKeyPair"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AutoScalingConsoleReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura all'Auto Scaling tramite. Console di gestione AWS

`AutoScalingConsoleReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AutoScalingConsoleReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2017, 19:48 UTC
- Ora modificata: 12 gennaio 2017, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AutoScalingFullAccess

Descrizione: Fornisce l'accesso completo all'Auto Scaling.

`AutoScalingFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AutoScalingFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2017, 19:31 UTC
- Ora modificata: 6 febbraio 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AutoScalingNotificationAccessRole

Descrizione: politica predefinita per il ruolo del servizio AutoScaling Notification Access.

`AutoScalingNotificationAccessRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AutoScalingNotificationAccessRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AutoScalingReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura all'Auto Scaling.

`AutoScalingReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AutoScalingReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2017, 19:39 UTC
- Ora modificata: 12 gennaio 2017, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AutoScalingServiceRolePolicy

Descrizione: Consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Auto Scaling

`AutoScalingServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 8 gennaio 2018, 23:10 UTC
- Ora modificata: 12 novembre 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateReplaceRootVolumeTask",
        "ec2:CreateFleet",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DetachClassicLinkVpc",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
```

```
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2InstanceProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ELBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Register*",
        "elasticloadbalancing:Deregister*",
        "elasticloadbalancing:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWManagement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSManagement",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerParameterManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeManagement",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeregisterTargets",
```

```
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListTargets",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:RegisterTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsManagement",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWS-SSM-Automation-DiagnosisBucketPolicy

Descrizione: fornisce le autorizzazioni per accedere al bucket SSM Diagnosis S3 per la diagnosi e la risoluzione dei problemi.

`AWS-SSM-Automation-DiagnosisBucketPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWS-SSM-Automation-DiagnosisBucketPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2024, 23:31 UTC
- Ora modificata: 15 novembre 2024, 23:31 UTC

- ARN: `arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

Descrizione: autorizza la diagnosi dei problemi con i servizi SSM eseguendo le attività definite in Automation Documents, utilizzate principalmente per eseguire i documenti di automazione in una configurazione interregionale tra account attivando automazioni secondarie all'interno degli account dei membri.

`AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 novembre 2024, 00:01 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

Descrizione: autorizza la diagnosi dei problemi con i servizi SSM eseguendo le attività definite in Automation Documents, utilizzate principalmente per eseguire i documenti di automazione in una account/region configurazione di destinazione diagnosticando lo stato del servizio SSM su tutti i nodi.

`AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 novembre 2024, 00:08 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeNetworkAcls"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationStepExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeActivations",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:automation-execution/*",
```

```
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

Descrizione: fornisce le autorizzazioni agli account operativi per diagnosticare i nodi non gestiti fornendo all'organizzazione le autorizzazioni specifiche richieste dall'automazione SSM per estrarre l'elenco degli account membri all'interno della radice di un'organizzazione per attivare l'esecuzione tra account e più regioni, consentendo l'assunzione di ruoli di esecuzione nell'account/regione di destinazione.

`AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 novembre 2024, 00:11 UTC
- Ora modificata: 16 novembre 2024, 00:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWS-SSM-RemediationAutomation-AdministrationRolePolicy

Descrizione: autorizza a risolvere i problemi con i servizi SSM eseguendo le attività definite nei documenti di automazione, utilizzate principalmente per eseguire i documenti di automazione in una configurazione interregionale tra account attivando automazioni secondarie all'interno degli account dei membri.

`AWS-SSM-RemediationAutomation-AdministrationRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWS-SSM-RemediationAutomation-AdministrationRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 novembre 2024, 00:14 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-AdministrationRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWS-SSM-RemediationAutomation-ExecutionRolePolicy

Descrizione: fornisce le autorizzazioni per risolvere i problemi con i servizi SSM eseguendo le attività definite in Automation Documents, utilizzate principalmente per eseguire i documenti di automazione in una account/region configurazione di destinazione correggendo l'integrità dei servizi SSM su tutti i nodi.

`AWS-SSM-RemediationAutomation-ExecutionRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWS-SSM-RemediationAutomation-ExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 novembre 2024, 00:17 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-ExecutionRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateVpcEndpointForTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "RestrictCreateVpcEndpointForSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.ssm",
            "com.amazonaws.*.ssmmessages",
            "com.amazonaws.*.ec2messages"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint"
        }
      }
    },
    {
      "Sid" : "RestrictCreateVpcEndpointWithTag",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint",
          "ec2:CreateAction" : [
            "CreateVpcEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "AllowModifyVpcAttributeForDns",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Attribute" : [
            "EnableDnsSupport",
            "EnableDnsHostnames"
          ]
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
```

```
      "Sid" : "AllowSecurityGroupRuleUpdateForTaggedResource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateTagRule",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess",
```

```
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupEgress",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateSecurityGroupForVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "AllowCreateSecurityGroupWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowTagCreationForSecurityGroupTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup",
```

```
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

Descrizione: fornisce le autorizzazioni agli account operativi per riparare i nodi non gestiti fornendo all'organizzazione le autorizzazioni specifiche richieste dall'automazione SSM per estrarre l'elenco degli account membri all'interno della radice di un'organizzazione per attivare l'esecuzione tra account e più regioni, consentendo l'assunzione di ruoli di esecuzione nell'account/regione di destinazione.

`AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 novembre 2024, 00:25 UTC
- Ora modificata: 16 novembre 2024, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWS_ ConfigRole

Descrizione: politica predefinita per il ruolo del servizio AWS Config. Fornisce le autorizzazioni necessarie a AWS Config per tenere traccia delle modifiche alle risorse. AWS

`AWS_ConfigRole`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWS_ConfigRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica relativa al ruolo del servizio
- Ora di creazione: 15 settembre 2020, 20:30 UTC
- Ora modificata: 30 luglio 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Versione della politica

Versione della politica: v71 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
```

```
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
```

```
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListTagsForResource",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
```

```
        "appsync:GetApi",
        "appsync:GetApiAssociation",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListGraphqlApis",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
```

```
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetControl",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
```

```
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-dashboards:GetDashboard",
        "bcm-dashboards:ListDashboards",
        "bcm-dashboards:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyEngineSummary",
        "bedrock-agentcore:GetPolicySummary",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGateways",
```

```
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyEngineSummaries",
        "bedrock-agentcore:ListPolicySummaries",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
```

```
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "chime:DescribeAppInstance",
        "chime:ListAppInstances",
        "chime:ListTagsForResource",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTables",
```

```
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListCachePolicies",
```

```
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListFunctions",
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListManagedInsightRules",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
```

```
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListFleets",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminGetUser",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
```

```
        "cognito-idp:DescribeManagedLoginBranding",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeEmailAddress",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
```

```
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeView",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListEvaluationFormVersions",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUsers",
        "connect:ListViews",
        "connect:ListViewVersions",
        "connect:SearchAvailablePhoneNumbers",
        "controltower:GetLandingZone",
        "controltower:ListLandingZones",
        "cur:DescribeReportDefinitions",
        "cur:ListTagsForResource",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
```

```
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
```

```
        "datazone:SearchUserProfiles",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetStorageProfile",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueues",
        "deadline:ListStorageProfiles",
        "deadline:ListTagsForResource",
        "detective:ListGraphs",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
```

```
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
```

```
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
```

```
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
```

```
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
```

```
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
```

```
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerFleet",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScalingPolicies",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
```

```
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeAcceleratorAttributes",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
```

```
        "glue:GetSession",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSessions",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:GetDeployment",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "greengrass:ListDeployments",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatEntitySet",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
```

```
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
```

```
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
```

```
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackages",
        "iot:ListPackageVersions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
```

```
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigRoleStatementID2",
      "Effect" : "Allow",
      "Action" : [
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle",
```

```
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
```

```
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
```

```
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra-ranking:ListTagsForResource",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
```

```
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
```

```
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "license-manager:ListTagsForResource",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
```

```
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
```

```
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNode",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListNodes",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
```

```
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mpa:GetIdentitySource",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
```

```
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "mq:ListTags",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "notifications:GetEventRule",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
```

```
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListSinks",
        "oam:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:ListAnnotationStores",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
```

```
        "outposts:GetSite",
        "outposts:ListSites",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
```

```
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetPolicy",
        "qbusiness:ListApplications",
        "qbusiness:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
```

```
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
```

```
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListCollections",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
```

```
        "robomaker:ListSimulationApplications",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
```

```
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rtbfabric:GetInboundExternalLink",
        "rtbfabric:GetLink",
        "rtbfabric:GetOutboundExternalLink",
        "rtbfabric:GetRequesterGateway",
        "rtbfabric:GetResponderGateway",
        "rtbfabric:ListLinks",
        "rtbfabric:ListRequesterGateways",
        "rtbfabric:ListResponderGateways",
        "rtbfabric:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
```

```
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
```

```
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:ListTableBuckets",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterSchedulerConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
```

```
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
```

```
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListClusters",
        "sagemaker:ListClusterSchedulerConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListMlflowApps",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardExportJobs",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListOptimizationJobs",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
```

```
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListTagsForResource",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
```

```
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serviceCatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:DescribeTagOption",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ListTagOptions",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
        "ses:ListArchives",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListIngressPoints",
```

```
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListRelays",
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:GetRotation",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListRotations",
```

```
        "ssm-contacts:ListTagsForResource",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListActivities",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "states:ListTagsForResource",
```

```
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "textract:GetAdapter",
        "textract:ListAdapters",
        "textract:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWebApp",
        "transfer:DescribeWebAppCustomization",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWebApps",
        "transfer:ListWorkflows",
        "verifiedpermissions:GetIdentitySource",
```

```
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
```

```
        "wisdom:GetAIGuardrail",
        "wisdom:ListAIGuardrails",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetSamplingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigLogStreamStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "ConfigLogEventsStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAccountActivityAccess

Descrizione: consente agli utenti di accedere alla pagina Attività dell'account.

`AWSAccountActivityAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAccountActivityAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 20 febbraio 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAccountManagementFullAccess

Descrizione: fornisce l'accesso completo alla gestione degli AWS account.

`AWSAccountManagementFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAccountManagementFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 settembre 2021, 23:20 UTC
- Ora modificata: 30 settembre 2021, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "account:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAccountManagementReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura alla gestione degli account AWS

`AWSAccountManagementReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAccountManagementReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 settembre 2021, 23:29 UTC
- Ora modificata: 30 settembre 2021, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:Get*",
        "account:List*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAccountSettingsManagementRole

Descrizione: fornisce le autorizzazioni necessarie per gestire un account per AWS le applicazioni.

`AWSAccountSettingsManagementRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAccountSettingsManagementRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2025, 17:49 UTC
- Ora modificata: 08 luglio 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountSettingsManagementRole`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:GetAccountInformation",
        "account:CloseAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "payments:ListTagsForResource",
        "payments:UntagResource",
        "payments:TagResource",
        "payments:ListPaymentPreferences",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:MakePayment",
        "payments:UpdatePaymentPreferences",
        "payments:CreatePaymentInstrument",
        "payments:UpdatePaymentInstrument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetSellerOfRecord"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tax:GetTaxRegistration",
        "tax:PutTaxRegistration",
        "tax:ListTaxRegistrations",
        "tax:DeleteTaxRegistration",
        "tax:BatchPutTaxRegistration",
        "tax:GetTaxRegistrationDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:UpdateCustomerVerificationDetails"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:ListApplications",
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAccountUsageReportAccess

Descrizione: consente agli utenti di accedere alla pagina del rapporto sull'utilizzo dell'account.

`AWSAccountUsageReportAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAccountUsageReportAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewUsage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAgentlessDiscoveryService

Descrizione: fornisce l'accesso al Discovery Agentless Connector per la registrazione con AWS Application Discovery Service.

`AWSAgentlessDiscoveryService`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAgentlessDiscoveryService` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 agosto 2016, 01:35 UTC
- Ora modificata: 24 febbraio 2020, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "awsconnector:RegisterConnector",
        "awsconnector:GetConnectorHealth"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade/*",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-connector-debug-logs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    },
    {
      "Sid" : "Discovery",
      "Effect" : "Allow",
```

```
      "Action" : [
        "Discovery:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "arsenal",
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppConfigServiceRolePolicy

Descrizione: consente di AWS AppConfig chiamare AWS i servizi per conto dell'utente.

`AWSAppConfigServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 8 maggio 2026, 18:42 UTC
- Ora modificata: 08 maggio 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppConfigServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPutExperimentMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppConfig"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppFabricFullAccess

Descrizione: fornisce l'accesso completo al AWS AppFabric servizio e l'accesso in sola lettura ai servizi dipendenti come S3, Kinesis, KMS.

`AWSAppFabricFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSAppFabricFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2023, 19:51 UTC
- Ora modificata: 27 giugno 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "appfabric:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FirehoseReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowUseOfServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appfabric.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppFabricReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS AppFabric

`AWSAppFabricReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAppFabricReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 27 giugno 2023, 19:52 UTC
- Ora modificata: 27 giugno 2023, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppFabricServiceRolePolicy

Descrizione: fornisce AppFabric l'accesso alle AWS risorse per tuo conto

`AWSAppFabricServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 giugno 2023, 21:07 UTC
- Ora modificata: 26 giugno 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEmitMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppFabric"
        }
      }
    },
    {
      "Sid" : "S3PutObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
```

```
      ],
      "Resource" : "arn:aws:s3:::*/AWSAppFabric/*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FirehosePutRecord",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AWSAppFabricManaged" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingAppStreamFleetPolicy

Descrizione: Politica che concede le autorizzazioni ad Application Auto Scaling per accedere e. AppStream CloudWatch

`AWSApplicationAutoscalingAppStreamFleetPolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 ottobre 2017, 19:04 UTC
- Ora modificata: 20 ottobre 2017, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingCassandraTablePolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere a Cassandra e. CloudWatch

`AWSApplicationAutoscalingCassandraTablePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 marzo 2020, 22:49 UTC
- Ora modificata: 18 marzo 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cassandra:Select",
      "Resource" : [
        "arn:*:cassandra:*:*:/keyspace/system/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema_mcs/table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Alter",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingComprehendEndpointPolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere a Comprehend and. CloudWatch

`AWSApplicationAutoscalingComprehendEndpointPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 novembre 2019, 18:39 UTC
- Ora modificata: 14 novembre 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoScalingCustomResourcePolicy

Descrizione: Policy che concede le autorizzazioni di APIGateway accesso ad Application Auto Scaling CloudWatch e per il ridimensionamento personalizzato delle risorse

`AWSApplicationAutoScalingCustomResourcePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 4 giugno 2018, 23:22 UTC
- Ora modificata: 04 giugno 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingDynamoDBTablePolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a DynamoDB e. CloudWatch

`AWSApplicationAutoscalingDynamoDBTablePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 ottobre 2017, 21:34 UTC
- Ora modificata: 20 ottobre 2017, 21:34 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a EC2 Spot Fleet e. CloudWatch

`AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 25 ottobre 2017, 18:23 UTC
- Ora modificata: 25 ottobre 2017, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingECSServicePolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a EC2 Container Service e. CloudWatch

`AWSApplicationAutoscalingECSServicePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 25 ottobre 2017, 23:53 UTC
- Ora modificata: 20 maggio 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:DescribeServiceRevisions",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingElastiCacheRGPolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere ad Amazon e Amazon ElastiCache . CloudWatch

`AWSApplicationAutoscalingElastiCacheRGPolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 agosto 2021, 23:41 UTC
- Ora modificata: 26 marzo 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheActionsOnAllClusters",
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeReplicationGroups",
        "elasticache:ModifyCacheCluster",
        "elasticache:ModifyReplicationGroupShardConfiguration",
        "elasticache:IncreaseReplicaCount",
        "elasticache:DecreaseReplicaCount",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingEMRInstanceGroupPolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a Elastic Map Reduce e. CloudWatch

`AWSApplicationAutoscalingEMRInstanceGroupPolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 26 ottobre 2017, 00:57 UTC
- Ora modificata: 26 ottobre 2017, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingKafkaClusterPolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a Managed Streaming for Apache Kafka e. CloudWatch

`AWSApplicationAutoscalingKafkaClusterPolicy`è una AWS politica gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 24 agosto 2020, 18:36 UTC
- Ora modificata: 24 agosto 2020, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingLambdaConcurrencyPolicy

Descrizione: policy che concede le autorizzazioni ad Application Auto Scaling per accedere a Lambda e. CloudWatch

`AWSApplicationAutoscalingLambdaConcurrencyPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 ottobre 2019, 20:04 UTC
- Ora modificata: 21 ottobre 2019, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingNeptuneClusterPolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere ad Amazon Neptune e Amazon. CloudWatch

`AWSApplicationAutoscalingNeptuneClusterPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 2 settembre 2021, 21:14 UTC
- Ora modificata: 2 settembre 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterParameters",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "rds:AddTagsToResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:CreateDBInstance",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*",
        "arn:aws:rds:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingRDSClusterPolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere a RDS e. CloudWatch

`AWSApplicationAutoscalingRDSClusterPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 ottobre 2017, 17:46 UTC
- Ora modificata: 07 agosto 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CreateDBInstance",
        "rds:DeleteDBInstance",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:ModifyDBCluster",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingSageMakerEndpointPolicy

Descrizione: Politica che concede le autorizzazioni ad Application Auto Scaling per accedere e. SageMaker CloudWatch

`AWSApplicationAutoscalingSageMakerEndpointPolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 6 febbraio 2018, 19:58 UTC
- Ora modificata: 13 novembre 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMaker",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationAutoscalingWorkSpacesPoolPolicy

Descrizione: politica che concede le autorizzazioni ad Application Auto Scaling per accedere ad Amazon e Amazon WorkSpaces . CloudWatch

`AWSApplicationAutoscalingWorkSpacesPoolPolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 giugno 2024, 18:39 UTC

- Ora modificata: 17 giugno 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingWorkSpacesPoolPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesActionsOnAllPools",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeWorkspacesPools",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationDiscoveryAgentAccess

Descrizione: fornisce l'accesso al Discovery Agent per la registrazione con AWS Application Discovery Service.

`AWSApplicationDiscoveryAgentAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationDiscoveryAgentAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2016, 21:38 UTC
- Ora modificata: 24 febbraio 2020, 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationDiscoveryAgentlessCollectorAccess

Descrizione: consente a Application Discovery Service Agentless Collector di aggiornare, registrare e comunicare automaticamente con Application Discovery Service

`AWSApplicationDiscoveryAgentlessCollectorAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationDiscoveryAgentlessCollectorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 agosto 2022, 21:00 UTC
- Ora modificata: 16 agosto 2022, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:DescribeImages"
      ],
      "Resource" : "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationDiscoveryServiceFullAccess

Descrizione: Fornisce l'accesso completo alla visualizzazione e all'etichettatura degli elementi di configurazione gestiti dall' AWS Application Discovery Service

`AWSApplicationDiscoveryServiceFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationDiscoveryServiceFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2016, 21:30 UTC
- Ora modificata: 19 giugno 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
```

```
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
```

```
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationAgentInstallationPolicy

Descrizione: questa politica consente di installare il AWS Replication Agent, che viene utilizzato con AWS Application Migration Service (MGN) per migrare server esterni verso. AWS Allega questa policy agli utenti o ai ruoli IAM di cui fornisci le credenziali durante l'installazione del Replication Agent. AWS

`AWSApplicationMigrationAgentInstallationPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationAgentInstallationPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 giugno 2022, 07:51 UTC
- Ora modificata: 20 settembre 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:VerifyClientRoleForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationAgentPolicy

Descrizione: questa policy consente l'installazione e l'utilizzo del AWS Replication Agent, utilizzato con AWS Application Migration Service (MGN) per migrare server esterni verso. AWS Allega questa policy agli utenti o ai ruoli IAM di cui fornisci le credenziali durante l'installazione del Replication Agent. AWS

`AWSApplicationMigrationAgentPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationAgentPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 aprile 2021, 07:00 UTC
- Ora modificata: 20 settembre 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationAgentPolicy_v2

Descrizione: questa policy consente di utilizzare il AWS Replication Agent, utilizzato con AWS Application Migration Service (MGN) per migrare server esterni verso. AWS Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

`AWSApplicationMigrationAgentPolicy_v2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationAgentPolicy_v2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 giugno 2022, 14:14 UTC
- Ora modificata: 06 giugno 2022, 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn",
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/${aws:SourceIdentity}"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationConversionServerPolicy

Descrizione: questa policy consente al server di conversione di Application Migration Service (MGN), che sono istanze EC2 lanciate da Application Migration Service, di comunicare con il servizio MGN. Un ruolo IAM con questa policy viene allegato (come profilo di istanza EC2) da MGN ai server di conversione MGN, che vengono avviati e terminati automaticamente da MGN, quando necessario. Non è consigliabile collegare questa policy ai propri utenti o ruoli IAM. I server di conversione MGN vengono utilizzati da Application Migration Service quando gli utenti scelgono di avviare istanze Test o Cutover utilizzando la console MGN, la CLI o l'API.

`AWSApplicationMigrationConversionServerPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationConversionServerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 07 aprile 2021, 06:48 UTC
- Ora modificata: 07 aprile 2021, 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationEC2Access

Descrizione: questa policy fornisce le operazioni di Amazon EC2 necessarie per utilizzare Application Migration Service (MGN) per avviare i server migrati come istanze EC2. Allega questa policy ai tuoi utenti o ruoli IAM.

`AWSApplicationMigrationEC2Access`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationEC2Access` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 07 aprile 2021, 07:05 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
```

```
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationFSxProxyPolicy

Descrizione: fornisce le autorizzazioni per gestire il file system ONTAP

`AWSApplicationMigrationFSxProxyPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationFSxProxyPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 31 maggio 2026, 13:12 UTC
- Ora modificata: 31 maggio 2026, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationFSxProxyPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxDescribe",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FSxCreateVolume",
      "Effect" : "Allow",
      "Action" : "fsx:CreateVolume",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxCreateVolumeSVM",
      "Effect" : "Allow",
      "Action" : "fsx:CreateVolume",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Sid" : "FSxTagging",
      "Effect" : "Allow",
      "Action" : [
        "fsx:TagResource",
```

```
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxUpdateAndDeleteVolume",
      "Effect" : "Allow",
      "Action" : [
        "fsx:UpdateVolume",
        "fsx:DeleteVolume"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationFSxProxyVPCPolicy

Descrizione: Fornisce le autorizzazioni per la gestione PrivateLink tra AWS Application Migration Service e il file system FSx del cliente

`AWSApplicationMigrationFSxProxyVPCPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationFSxProxyVPCPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 31 maggio 2026, 13:27 UTC
- Ora modificata: 31 maggio 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationFSxProxyVPCPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowlistAllVPCsforSGCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateServiceEndpointResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/file_system_id" : "false",
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "EC2AllowOperationsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVpcEndpointServiceConfigurations"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/file_system_id" : "false",
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:GetSecurityGroupsForVpc",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "ec2:DescribeInternetGateways",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyVpcEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:AcceptVpcEndpointConnections"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/file_system_id" : "false",
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "EC2AllowTaggingOnCreate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVpcEndpointServiceConfiguration"
          ]
        }
      }
    },
    {
      "Sid" : "CreateFSxNLB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
```

```
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*NLB/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/file_system_id" : "false",
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxNLBAllowTaggingOnCreate",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*NLB/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*TG/*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/MgnFSxProxy*/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateTargetGroup",
            "CreateListener"
          ]
        }
      }
    },
    {
      "Sid" : "FSxNLBRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "RegisterFSxTargetGroup",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:RegisterTargets",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*/*"
    },
    {
      "Sid" : "ELBv2AllowModify",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyLoadBalancerAttributes",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*/*"
    },
    {
      "Sid" : "ELBv2AllowOperationsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/MgnFSxProxy*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/file_system_id" : "false",
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationFullAccess

Descrizione: questa policy fornisce le autorizzazioni a tutte le API pubbliche di AWS Application Migration Service (MGN), nonché le autorizzazioni per leggere le informazioni chiave del KMS. Allega questa policy ai tuoi utenti o ruoli IAM.

`AWSApplicationMigrationFullAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 07 aprile 2021, 06:56 UTC
- Ora modificata: 3 agosto 2026, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Versione della politica

Versione della politica: v14 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor4",
```

```
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : "iam:ListInstanceProfiles",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ],
```

```
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "drs:DisconnectSourceServer"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    },
    {
      "Sid" : "VisualEditor14",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor15",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
    },
    {
      "Sid" : "VisualEditor16",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ]
    },
    {
      "Sid" : "VisualEditor17",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor18",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSMigration-*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "mgn.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "VisualEditor19",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommands",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor20",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FSxReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowTagSVMWithMapKeys",
      "Effect" : "Allow",
      "Action" : [
        "fsx:TagResource"
      ],
```

```
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "map-migrated",
            "aws-apn-id"
          ]
        }
      }
    },
    {
      "Sid" : "FSxDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes",
        "fsx:DescribeSnapshots"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FSxCreateVolume",
      "Effect" : "Allow",
      "Action" : "fsx:CreateVolume",
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "FSxDeleteVolumeAndTag",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FSxCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:CreateSnapshot",
      "Resource" : [
        "arn:aws:fsx:*:*:snapshot/*/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationMGHAccess

Descrizione: questa politica consente all' AWS Application Migration Service (MGN) di inviare metadati sullo stato di avanzamento dei server in fase di migrazione tramite MGN a Migration AWS Hub (MGH). MGN crea automaticamente un ruolo IAM con questa policy allegata e assume questo ruolo. Non è consigliabile collegare questa policy ai propri utenti o ruoli IAM.

`AWSApplicationMigrationMGHAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationMGHAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 aprile 2021, 07:10 UTC
- Ora modificata: 07 aprile 2021, 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationNetworkMigrationCustomResource

Descrizione: fornisce le autorizzazioni per la risorsa personalizzata Network Migration

`AWSApplicationMigrationNetworkMigrationCustomResource`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationNetworkMigrationCustomResource` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 novembre 2025, 11:34 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationCustomResource`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ModifyTGW",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationNetworkMigrationMultiAccount

Descrizione: fornisce le autorizzazioni per automatizzare la migrazione da VMware all' AWS infrastruttura di rete tramite CloudFormation

`AWSApplicationMigrationNetworkMigrationMultiAccount`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationNetworkMigrationMultiAccount` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 novembre 2025, 09:04 UTC
- Ora modificata: 30 luglio 2026, 07:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationMultiAccount`

Versione della politica

Versione della politica: v6 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2CFNReadonlyPrefixList",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:prefix-list/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "NetworkAnalyzer",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreatePermissionsByCFNNACL",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFNNACLSN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "EC2CFNReadonly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "MGNCFNDescribe",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*"
    },
    {
      "Sid" : "CFNCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    },
    {
      "Sid" : "CFNOperations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNProvision",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2PutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
```

```
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2RequestSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2SecurityGroupTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "EC2TagCFNSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
```

```
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateNatGateway",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:natgateway/*",
```

```
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AllowCreateTGWVpcAttachmentSameOrg",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    },
    {
      "Sid" : "CFNProvisionNetworking",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateVpc",
        "ec2:CreateTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:transit-gateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworking",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagRouting",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNAT",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTransitGateway",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTGWAttachment",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
```

```
      "Sid" : "CreatePermissionsByRequestTagNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "DeleteENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagInsights",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-insights-path/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
```

```
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "EC2TagCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateTransitGatewayVpcAttachment",
            "CreateTransitGatewayRouteTableAnnouncement",
            "CreateTransitGatewayRouteTable",
            "CreateTransitGatewayRoute",
            "CreateTransitGatewayPrefixListReference",
            "CreateTransitGatewayPolicyTable",
            "CreateTransitGatewayPeeringAttachment",
            "CreateTransitGatewayConnectPeer",
            "CreateTransitGatewayConnect",
```

```
            "CreateTransitGateway",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateSubnet",
            "CreateNetworkAcl",
            "CreateRouteTable",
            "CreateNetworkInterface",
            "CreateNetworkInsightsPath",
            "CreateNetworkInsightsAccessScope",
            "CreateLaunchTemplate",
            "AllocateAddress",
            "StartNetworkInsightsAnalysis",
            "CreateVpc"
          ]
        }
      }
    },
    {
      "Sid" : "deployerWorkload",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "putParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "deleteParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:DeleteResourcePolicy",
        "ssm:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "ramResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutResourcePolicy",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ramTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreateResourceShareTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "Bool" : {
          "ram:RequestedAllowsExternalPrincipals" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
```

```
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AssociateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "ram:RequestedResourceType" : [
            "ec2:TransitGateway",
            "ssm:Parameter"
          ]
        }
      }
    },
    {
      "Sid" : "CreateResourceShareWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
```

```
      }
    },
    {
      "Sid" : "AllowGetResourceShares",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*"
    },
    {
      "Sid" : "CreateCustomResourceLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/network-migration-modify-tgw*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "GetCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OperationsCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreateRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "PassGetRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OperationsRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AttachCustomResourceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
```

```
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/
AWSApplicationMigrationNetworkMigrationCustomResource"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "MGNCFNBasedResourcesProvision",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateNatGatewayAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
```

```
        "ec2:DeleteSubnet",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateNatGatewayAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyLaunchTemplate",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:ModifyVolume",
        "ec2:ModifyVpcAttribute",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
```

```
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerENIResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationReadOnlyAccess

Descrizione: questa policy fornisce le autorizzazioni per tutte le API pubbliche di sola lettura di Application Migration Service (MGN), nonché per alcune API di sola lettura di altri AWS servizi necessarie per utilizzare appieno la console MGN in sola lettura. Allega questa policy ai tuoi utenti o ruoli IAM.

`AWSApplicationMigrationReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 aprile 2021, 07:15 UTC
- Ora modificata: 01 luglio 2026, 14:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeSourceServers",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:GetLaunchConfiguration",
        "mgn:DescribeVcenterClients",
        "mgn:GetReplicationConfiguration",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListApplications",
        "mgn:ListWaves",
        "mgn:ListExports",
        "mgn:ListImports",
        "mgn:ListImportErrors",
        "mgn:ListExportErrors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationReplicationServerPolicy

Descrizione: questa policy consente ai server di replica di Application Migration Service (MGN), che sono istanze EC2 lanciate da Application Migration Service, di comunicare con il servizio MGN e di creare istantanee EBS all'interno dell'utente. Account AWS Un ruolo IAM con questa policy è associato (come profilo di istanza EC2) da Application Migration Service ai server di replica MGN, che vengono avviati e terminati automaticamente da MGN, in base alle esigenze. I server di replica MGN vengono utilizzati per facilitare la replica dei dati dai server esterni a AWS, come parte del processo di migrazione gestito tramite MGN. Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

`AWSApplicationMigrationReplicationServerPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationReplicationServerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 7 aprile 2021, 07:21 UTC
- Ora modificata: 31 maggio 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn",
        "mgn:GetAgentSnapshotCreditsForMgn",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSnapshotRequestsForMgn",
        "mgn:BatchDeleteSnapshotRequestForMgn",
        "mgn:NotifyAgentAuthenticationForMgn",
        "mgn:BatchCreateVolumeSnapshotGroupForMgn",
        "mgn:UpdateAgentReplicationProcessStateForMgn",
        "mgn:NotifyAgentReplicationProgressForMgn",
        "mgn:NotifyAgentConnectedForMgn",
        "mgn:NotifyAgentDisconnectedForMgn",
        "mgn:StartSnapshotGroupForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationServiceEc2InstancePolicy

Descrizione: questa policy consente l'installazione e l'utilizzo del AWS Replication Agent, utilizzato da AWS Application Migration Service (AWS MGN) per migrare i server di origine eseguiti su EC2 (Cross-region o Cross-AZ). Un ruolo IAM con questa policy deve essere allegato (come profilo di istanza EC2) alle istanze EC2.

`AWSApplicationMigrationServiceEc2InstancePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationServiceEc2InstancePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 agosto 2023, 13:19 UTC
- Ora modificata: 03 gennaio 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MgnAgentInstallation",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:GetAgentInstallationAssetsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MgnAgentReplication",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Sid" : "MgnSourceServerTagResource",
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationServiceRolePolicy

Descrizione: consente all' AWS Application Migration Service di creare e gestire AWS risorse per conto dell'utente.

`AWSApplicationMigrationServiceRolePolicy`è una policy AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 07 aprile 2021, 06:43 UTC
- Ora modificata: 19 luglio 2026, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Versione della politica

Versione della politica: v9 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVolumes",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "RegisterImage"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationSSMAccess

Descrizione: questa policy fornisce l'accesso alle operazioni di Amazon SSM necessarie per utilizzare Application Migration Service (MGN) per eseguire documenti SSM con comandi post-migrazione personalizzati. Allega questa policy ai tuoi utenti o ruoli IAM.

`AWSApplicationMigrationSSMAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationSSMAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 09:29 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSApplicationMigrationVCenterClientPolicy

Descrizione: questa politica consente l'installazione e l'utilizzo del AWS VCenter Client, che viene utilizzato con AWS Application Migration Service (MGN) per migrare server esterni verso. AWS Allega questa policy agli utenti o ai ruoli IAM di cui fornisci le credenziali durante l'installazione del Client. AWS VCenter

`AWSApplicationMigrationVCenterClientPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSApplicationMigrationVCenterClientPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 08 novembre 2021, 12:53 UTC
- Ora modificata: 08 novembre 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateVcenterClientForMgn",
        "mgn:DescribeVcenterClients"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetVcenterClientCommandsForMgn",
        "mgn:SendVcenterClientCommandResultForMgn",
        "mgn:SendVcenterClientLogsForMgn",
        "mgn:SendVcenterClientMetricsForMgn",
        "mgn:DeleteVcenterClient",
        "mgn:TagResource",
        "mgn:NotifyVcenterClientStartedForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:vcenter-client/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppMeshEnvoyAccess

Descrizione: policy di App Mesh Envoy per l'accesso alla configurazione del nodo virtuale.

`AWSAppMeshEnvoyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAppMeshEnvoyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 luglio 2019, 21:29 UTC
- Ora modificata: 03 luglio 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:StreamAggregatedResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppMeshFullAccess

Descrizione: fornisce l'accesso completo all' AWS App Mesh APIs e alla console di gestione.

`AWSAppMeshFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAppMeshFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 aprile 2019, 17:50 UTC
- Ora modificata: 07 gennaio 2021, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appmesh.amazonaws.com/
AWSServiceRoleForAppMesh",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "appmesh.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppMeshPreviewEnvoyAccess

Descrizione: policy di App Mesh Preview Envoy per l'accesso alla configurazione del nodo virtuale.

`AWSAppMeshPreviewEnvoyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAppMeshPreviewEnvoyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 agosto 2019, 23:32 UTC
- Ora modificata: 5 agosto 2019, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh-preview:StreamAggregatedResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppMeshPreviewServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da AWS App Mesh

`AWSAppMeshPreviewServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 giugno 2019, 19:07 UTC

- Ora modificata: 21 agosto 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppMeshReadOnly

Descrizione: fornisce l'accesso in sola lettura all' AWS App Mesh APIs e alla console di gestione.

`AWSAppMeshReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAppMeshReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 aprile 2019, 17:51 UTC
- Ora modificata: 07 gennaio 2021, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:Describe*",
        "appmesh:List*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppMeshServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da AWS AppMesh

`AWSAppMeshServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 3 giugno 2019, 18:30 UTC
- Ora modificata: 10 ottobre 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppRunnerFullAccess

Descrizione: concede le autorizzazioni a tutte le azioni di App Runner.

`AWSAppRunnerFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSAppRunnerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 gennaio 2022, 04:02 UTC
- Ora modificata: 11 gennaio 2022, 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/apprunner.amazonaws.com/
AWSServiceRoleForAppRunner",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRunnerAdminAccess",
      "Effect" : "Allow",
      "Action" : "apprunner:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppRunnerReadOnlyAccess

Descrizione: concede le autorizzazioni per elencare e visualizzare i dettagli sulle risorse di App Runner.

`AWSAppRunnerReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSAppRunnerReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 febbraio 2022, 21:24 UTC
- Ora modificata: 24 febbraio 2022, 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apprunner:List*",
        "apprunner:Describe*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppRunnerServicePolicyForECRAccess

Descrizione: policy del servizio AWS App Runner che concede autorizzazioni di lettura alle risorse Amazon ECR nell'account del cliente. Usala in un ruolo che viene passato ad App Runner durante la creazione o l'aggiornamento di un servizio App Runner.

`AWSAppRunnerServicePolicyForECRAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAppRunnerServicePolicyForECRAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 maggio 2021, 19:17 UTC
- Ora modificata: 14 maggio 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppSyncAdministrator

Descrizione: fornisce l'accesso amministrativo al AppSync servizio, anche se non sufficiente per l'accesso tramite la console.

`AWSAppSyncAdministrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAppSyncAdministrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 marzo 2018, 21:20 UTC
- Ora modificata: 04 novembre 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "appsync.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appsync.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appsync.amazonaws.com/
AWSServiceRoleForAppSync*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppSyncInvokeFullAccess

Descrizione: fornisce l'accesso completo al AppSync servizio tramite invocazione, sia tramite la console che in modo indipendente

`AWSAppSyncInvokeFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAppSyncInvokeFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 marzo 2018, 21:21 UTC
- Ora modificata: 20 marzo 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppSyncPushToCloudWatchLogs

Descrizione: consente di AppSync inviare i log all' CloudWatch account dell'utente.

`AWSAppSyncPushToCloudWatchLogs`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAppSyncPushToCloudWatchLogs` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 09 aprile 2018, 19:38 UTC
- Ora modificata: 09 aprile 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppSyncSchemaAuthor

Descrizione: fornisce l'accesso per creare, aggiornare e interrogare lo schema.

`AWSAppSyncSchemaAuthor`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSAppSyncSchemaAuthor` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 marzo 2018, 21:21 UTC
- Ora modificata: 01 febbraio 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetResolver",
        "appsync:GetType",
        "appsync:GetDataSource",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetIntrospectionSchema",
        "appsync:GetGraphqlApi",
        "appsync:ListTypes",
        "appsync:ListApiKeys",
        "appsync:ListResolvers",
        "appsync:ListDataSources",
        "appsync:ListGraphqlApis",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:UntagResource",
        "appsync:ListTagsForResource",
        "appsync:CreateFunction",
        "appsync:UpdateFunction",
        "appsync:GetFunction",
        "appsync:DeleteFunction",
        "appsync:ListFunctions",
        "appsync:ListResolversByFunction",
        "appsync:EvaluateMappingTemplate",
        "appsync:EvaluateCode"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAppSyncServiceRolePolicy

Descrizione: consente l'accesso ai AWS servizi e alle risorse utilizzati o gestiti da AppSync

`AWSAppSyncServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 gennaio 2020, 19:56 UTC
- Ora modificata: 21 gennaio 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSArtifactAccountSync

Descrizione: consente AWS l'accesso in sola lettura di Artifact alle operazioni in Organizations. AWS

`AWSArtifactAccountSync`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSArtifactAccountSync` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 aprile 2018, 23:04 UTC
- Ora modificata: 10 aprile 2018, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSArtifactAgreementsFullAccess

Descrizione: Questa politica concede le autorizzazioni complete per elencare, scaricare, accettare e terminare gli accordi AWS Artifact. Include anche le autorizzazioni per elencare e abilitare l'accesso al AWS servizio nel servizio Organizzazione, oltre a descrivere i dettagli dell'organizzazione. Inoltre, la policy offre la possibilità di verificare se il ruolo collegato al servizio richiesto esiste e di crearne uno in caso contrario

`AWSArtifactAgreementsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSArtifactAgreementsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 novembre 2024, 19:36 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetAgreement",
```

```
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource" : "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid" : "CustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRoleToCheckForRoleExistence",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid" : "EnableServiceTrust",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EnableServiceTrustForArtifact",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "aws-artifact-account-sync.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSArtifactAgreementsReadOnlyAccess

Descrizione: Questa politica garantisce l'accesso in sola lettura all'elenco degli accordi di servizio Artifact e al AWS download degli accordi accettati. Include anche le autorizzazioni per elencare e descrivere i dettagli dell'organizzazione. Inoltre, la policy offre la possibilità di verificare se esiste il ruolo collegato al servizio richiesto.

`AWSArtifactAgreementsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSArtifactAgreementsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 novembre 2024, 19:36 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementsActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetCustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement"
      ],
```

```
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "AWSOrganizationActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSArtifactComplianceInquiriesFullAccess

Descrizione: fornisce l'accesso completo all'Artifact Compliance Inquiry.

`AWSArtifactComplianceInquiriesFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSArtifactComplianceInquiriesFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 giugno 2026, 19:27 UTC
- Ora modificata: 23 luglio 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactComplianceInquiriesFullAccess`

Versione della politica

Versione della politica: v2 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAndCreateComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListComplianceInquiries",
        "artifact:CreateComplianceInquiry"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListComplianceInquiryQueries",
        "artifact:GetComplianceInquiryMetadata",
        "artifact:ExportComplianceInquiry",
        "artifact:PutComplianceInquiryFeedback"
      ],
      "Resource" : "arn:aws:artifact:*:*:compliance-inquiry/*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSArtifactComplianceInquiriesReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a Artifact Compliance Inquiry.

`AWSArtifactComplianceInquiriesReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSArtifactComplianceInquiriesReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 giugno 2026, 19:42 UTC
- Ora modificata: 30 giugno 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactComplianceInquiriesReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListComplianceInquiries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetComplianceInquiryMetadata",
        "artifact:ListComplianceInquiryQueries",
        "artifact:ExportComplianceInquiry"
      ],
      "Resource" : "arn:aws:artifact:*:*:compliance-inquiry/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSArtifactReportsReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ai report del servizio Artifact AWS .

`AWSArtifactReportsReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSArtifactReportsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 gennaio 2024, 22:42 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "artifact:ListReportVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSArtifactServiceRolePolicy

Descrizione: consente a AWS Artifact di raccogliere informazioni su un'organizzazione tramite AWS il servizio Organizations.

`AWSArtifactServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 agosto 2023, 20:27 UTC
- Ora modificata: 21 agosto 2023, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAuditManagerAdministratorAccess

Descrizione: Fornisce l'accesso amministrativo per abilitare o disabilitare AWS Audit Manager, aggiornare le impostazioni e gestire valutazioni, controlli e framework

`AWSAuditManagerAdministratorAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSAuditManagerAdministratorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2020, 20:02 UTC
- Ora modificata: 15 maggio 2024, 23:46 UTC

- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
```

```
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "auditmanager.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "auditmanager.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMAccessManageSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:UpdateRoleDescription",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"
```

```
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ControlCatalogAccess",
      "Effect" : "Allow",
      "Action" : [
        "controlcatalog:ListCommonControls",
```

```
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAuditManagerServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da AWS Audit Manager

`AWSAuditManagerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 08 dicembre 2020, 15:12 UTC
- Ora modificata: 02 giugno 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListModelCustomizationJobs",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeContinuousBackups",
```

```
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:GetLaunchTemplateData",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
```

```
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
        "events:DescribeRule",
        "events:ListConnections",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccessKeyLastUsed",
        "iam:GetCredentialReport",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupsForUser",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListAccessKeys",
        "iam:ListAttachedRolePolicies",
        "iam:ListMfaDeviceTags",
        "iam:ListMfaDevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
```

```
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "es:DescribeDomains",
        "es:DescribeDomain",
        "es:DescribeDomainConfig",
        "es:ListDomainNames",
        "organizations:DescribeOrganization",
        "organizations:DescribePolicy",
        "organizations:DescribeAccount",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeLoggingStatus",
        "route53:GetQueryLoggingConfig",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
```

```
            "sagemaker:DescribeLabelingJob",
            "sagemaker:DescribeModel",
            "sagemaker:DescribeTrainingJob",
            "sagemaker:DescribeUserProfile",
            "sagemaker:ListAlgorithms",
            "sagemaker:ListDomains",
            "sagemaker:ListEndpoints",
            "sagemaker:ListEndpointConfigs",
            "sagemaker:ListFlowDefinitions",
            "sagemaker:ListHumanTaskUis",
            "sagemaker:ListLabelingJobs",
            "sagemaker:ListModels",
            "sagemaker:ListModelBiasJobDefinitions",
            "sagemaker:ListModelCards",
            "sagemaker:ListModelQualityJobDefinitions",
            "sagemaker:ListMonitoringAlerts",
            "sagemaker:ListMonitoringSchedules",
            "sagemaker:ListTrainingJobs",
            "sagemaker:ListUserProfiles",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketVersioning",
            "s3:GetEncryptionConfiguration",
            "s3:GetLifecycleConfiguration",
            "s3:ListAllMyBuckets",
            "secretsmanager:DescribeSecret",
            "secretsmanager:ListSecrets",
            "securityhub:DescribeStandards",
            "sns:ListTagsForResource",
            "sns:ListTopics",
            "sqs:ListQueues",
            "waf-regional:GetRule",
            "waf-regional:GetWebAcl",
            "waf:GetRule",
            "waf:GetRuleGroup",
            "waf:ListActivatedRulesInRuleGroup",
            "waf:ListWebAcls",
            "wafv2:ListWebAcls",
            "waf-regional:GetLoggingConfiguration",
            "waf-regional:ListRuleGroups",
            "waf-regional:ListSubscribedRuleGroups",
            "waf-regional:ListWebACLs",
            "waf-regional:ListRules",
            "waf:ListRuleGroups",
            "waf:ListRules"
```

```
      ],
      "Resource" : "*",
      "Sid" : "APIsAccess"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLogging",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEventsAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported",
          "events:source" : [
            "aws.securityhub"
          ]
        },
        "Null" : {
          "events:source" : "false",
          "events:detail-type" : "false"
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSAutoScalingPlansEC2AutoScalingPolicy

Descrizione: politica che concede le autorizzazioni ad Auto AWS Scaling per prevedere periodicamente la capacità e generare azioni di scaling pianificate per i gruppi di Auto Scaling in un piano di scalabilità

`AWSAutoScalingPlansEC2AutoScalingPolicy`è una AWS politica gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 23 agosto 2018, 22:46 UTC
- Ora modificata: 23 agosto 2018, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupAuditAccess

Descrizione: questa politica concede agli utenti le autorizzazioni per creare controlli e framework che definiscono le loro aspettative per le risorse e le attività di AWS Backup e per controllare le risorse e le attività di AWS Backup rispetto ai controlli e ai framework definiti. Questa politica concede le autorizzazioni a AWS Config e servizi simili per descrivere le aspettative degli utenti, eseguire gli audit. Questa politica concede anche le autorizzazioni per fornire report di controllo a S3 e servizi simili e consente agli utenti di trovare e aprire i propri report di controllo.

`AWSBackupAuditAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSBackupAuditAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 agosto 2021, 01:02 UTC
- Ora modificata: 10 aprile 2023, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateFramework",
        "backup:UpdateFramework",
        "backup:ListFrameworks",
        "backup:DescribeFramework",
        "backup:DeleteFramework",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:CreateReportPlan",
        "backup:UpdateReportPlan",
        "backup:ListReportPlans",
        "backup:DescribeReportPlan",
        "backup:DeleteReportPlan",
        "backup:StartReportJob",
        "backup:ListReportJobs",
        "backup:DescribeReportJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeComplianceByConfigRule"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupDataTransferAccess

Descrizione: questa politica consente all'agente AWS Backint di completare il trasferimento dei dati di backup con il piano AWS Backup Storage. Associa questa policy ai ruoli assunti dalle istanze EC2 che eseguono SAP HANA con l'agente Backint.

`AWSBackupDataTransferAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSBackupDataTransferAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 10 novembre 2022, 22:48 UTC
- Ora modificata: 10 novembre 2022, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:StartObject",
        "backup-storage:PutChunk",
        "backup-storage:GetChunk",
        "backup-storage:ListChunks",
        "backup-storage:ListObjects",
        "backup-storage:GetObjectMetadata",
        "backup-storage:NotifyObjectComplete"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupFullAccess

Descrizione: questa politica è destinata agli amministratori di backup e garantisce l'accesso completo alle operazioni di AWS backup, inclusa la creazione o la modifica dei piani di backup, l'assegnazione di AWS risorse ai piani di backup, l'eliminazione dei backup e il ripristino dei backup.

`AWSBackupFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSBackupFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 novembre 2019, 22:21 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Versione della politica

Versione della politica: v30 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RdsDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDbPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDbDeleteBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EfsFileSystemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "Ec2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2DeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ResourceGroupTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
```

```
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayGatewayStarPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AwsOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:backup:backup-vault"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemManagerCommandPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SystemManagerSendCommandPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:DescribeBackups",
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DirectoryServicePermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "IamCreateServiceLinkedRolePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BackupGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:AssociateGatewayToServer",
        "backup-gateway:CreateGateway",
        "backup-gateway:DeleteGateway",
        "backup-gateway:DeleteHypervisor",
        "backup-gateway:DisassociateGatewayFromServer",
        "backup-gateway:ImportHypervisorConfiguration",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup-gateway:PutMaintenanceStartTime",
        "backup-gateway:TagResource",
        "backup-gateway:TestHypervisorConfiguration",
        "backup-gateway:UntagResource",
        "backup-gateway:UpdateGatewayInformation",
        "backup-gateway:UpdateHypervisor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:PutHypervisorPropertyMappings",
        "backup-gateway:StartVirtualMachinesMetadataSync"
      ],
```

```
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayVirtualMachinePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:PutBandwidthRateLimitSchedule"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListTables",
        "timestream:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeletetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SystemsManagerForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceAccessManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
```

```
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Descrizione: fornisce AWS BackupGateway l'autorizzazione a sincronizzare i metadati delle macchine virtuali per tuo conto

`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 15 dicembre 2022, 19:43 UTC
- Ora modificata: 15 dicembre 2022, 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListVmTags",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "VMTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:TagResource",
        "backup-gateway:UntagResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupGuardDutyRolePolicyForScans

Descrizione: Fornisce GuardDuty l'autorizzazione a leggere i punti di AWS backup e ripristino per le scansioni di malware

`AWSBackupGuardDutyRolePolicyForScans`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBackupGuardDutyRolePolicyForScans` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2025, 03:34 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupGuardDutyRolePolicyForScans`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:ListChangedBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "CreateGrantForEncryptedVolumeCreation",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:guardduty:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
```

```
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "CreateGrantForReEncryptAndEBSDirect",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ShareSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : [
            "vol-*",
            "snap-*"
          ],
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupAccessPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
```

```
    },
    {
      "Sid" : "ReadAndDeleteBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupAccessPoint",
        "backup:DeleteBackupAccessPoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupRecoveryPointApiPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
    },
    {
      "Sid" : "DecryptKMSEncryptedDataByAWSBackup",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:backup:backup-vault" : "*",
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupOperatorAccess

Descrizione: questa politica concede agli utenti le autorizzazioni per assegnare AWS risorse ai piani di backup, creare backup su richiesta e ripristinare i backup. Questa politica non consente all'utente di creare o modificare piani di backup o di eliminare i backup pianificati dopo la creazione.

`AWSBackupOperatorAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBackupOperatorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 novembre 2019, 22:23 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Versione della politica

Versione della politica: v28 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:CreateBackupSelection",
```

```
        "backup:DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob",
        "backup:StartScanJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
```

```
    },
    {
      "Sid" : "EC2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewaySCSIAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayDiskReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayVolumeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMComandAccess",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FSXDescribeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FSxFileAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FSxVolumeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*"
    },
    {
      "Sid" : "FSxMachineAccess",
```

```
      "Effect" : "Allow",
      "Action" : "fsx:DescribeStorageVirtualMachines",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Sid" : "DirectoryServiceAccess",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayListAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayMachineAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway"
```

```
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamListAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftOptionsAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
```

```
    },
    {
      "Sid" : "CloudFormationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SAPAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SAPDatabaseAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupOrganizationAdminAccess

Descrizione: questa policy è destinata agli amministratori di backup che utilizzano la gestione dei backup tra account per gestire i backup per l'organizzazione.

`AWSBackupOrganizationAdminAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSBackupOrganizationAdminAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2020, 16:23 UTC
- Ora modificata: 18 novembre 2022, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DisableAWSServiceAccess",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DetachPolicy",
        "organizations:DisablePolicyType",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListPolicies",
        "organizations:EnablePolicyType",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : [
            "BACKUP_POLICY"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupRestoreAccessForSAPHANA

Descrizione: Fornisce l'autorizzazione di AWS backup per ripristinare un backup di SAP HANA su Amazon EC2

`AWSBackupRestoreAccessForSAPHANA`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSBackupRestoreAccessForSAPHANA` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 novembre 2022, 22:43 UTC
- Ora modificata: 10 novembre 2022, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:StartBackupJob",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:RestoreDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupSearchOperatorAccess

Descrizione: il ruolo di operatore di ricerca ha accesso alla creazione di indici di backup, alla creazione di ricerche di metadati di backup che sono stati indicizzati. Questa politica contiene le autorizzazioni necessarie per queste funzioni dell'operatore di ricerca.

`AWSBackupSearchOperatorAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBackupSearchOperatorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 febbraio 2025, 21:52 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/AWSBackupSearchOperatorAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartSearchAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchJob",
        "backup-search:ListSearchJobs",
        "backup-search:ListSearchResultExportJobs",
        "backup:ListIndexedRecoveryPointsForSearch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupSearchRecoveryPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:SearchRecoveryPoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:backup:*:*:recovery-point:*"
      ]
    },
    {
      "Sid" : "SearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchResultExportJob",
```

```
        "backup-search:StopSearchJob",
        "backup-search:GetSearchJob",
        "backup-search:GetSearchResultExportJob",
        "backup-search:ListSearchJobResults",
        "backup-search:ListSearchJobBackups"
      ],
      "Resource" : [
        "arn:aws:backup-search:*:*:search-job/*",
        "arn:aws:backup-search:*:*:search-export-job/*"
      ]
    },
    {
      "Sid" : "KMSDataKeyForSearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:backup-search:search-job"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "backup.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupServiceLinkedRolePolicyForBackup

Descrizione: Fornisce l'autorizzazione AWS di Backup per creare backup per conto dell'utente su tutti AWS i servizi

`AWSBackupServiceLinkedRolePolicyForBackup`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 2 giugno 2020, 23:08 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Versione della politica

Versione della politica: v31 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
```

```
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Sid" : "EC2CreateBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSBackupManagedResource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2RDSDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeImages",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBClusterSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CopyImage",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "RDSInstanceAndSnashotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBSnapshot",
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBInstanceAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSSnapshotTenantDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource"
```

```
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot-tenant-database:awsbackup:*"
      ]
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CopyBackup",
        "fsx:TagResource",
        "fsx:DescribeBackups",
        "fsx:DeleteBackup"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamoDBDeletePermissions",
      "Effect" : "Allow",
      "Action" : "dynamodb:DeleteBackup",
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "BackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListTagsForBackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTable"
      ],
```

```
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EventBridgePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:UpdateHANABackupSettings"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeTable",
        "timestream:GetAwsBackupStatus",
        "timestream:GetAwsRestoreStatus"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
```

```
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeleteSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrgsListDelegatedAdmins",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupServiceLinkedRolePolicyForBackupTest

Descrizione: Fornisce l'autorizzazione AWS di Backup per creare backup per conto dell'utente su tutti AWS i servizi

`AWSBackupServiceLinkedRolePolicyForBackupTest`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 maggio 2020, 17:37 UTC
- Ora modificata: 12 maggio 2020, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Effect" : "Allow",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupServiceRolePolicyForBackup

Descrizione: Fornisce l'autorizzazione AWS di Backup per creare backup per conto dell'utente su tutti AWS i servizi

`AWSBackupServiceRolePolicyForBackup`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBackupServiceRolePolicyForBackup` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 gennaio 2019, 21:01 UTC
- Ora modificata: 23 febbraio 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Versione della politica

Versione della politica: v30 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
```

```
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSInstanceAutomatedBackupPermissions",
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBInstanceAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:auto-backup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RDSClusterBackupPermissions",
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBClusterAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
    },
    {
      "Sid" : "RDSModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "RDSBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute"
```

```
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "RDSClusterModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSTagAndDeletePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:image/*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "EBSSnapshotTierPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "BackupVaultPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource" : "arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Sid" : "BackupVaultCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CopyFromBackupVault"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EBSResourcePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSDynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSEC2Permissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:ebs:id"
        }
      }
    },
    {
      "Sid" : "GetResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSendPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
```

```
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxCreateBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:CreateBackup",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxListTagsPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:ListTagsForResource",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
```

```
      "Sid" : "FsxResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:CopyBackup",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamodbBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:StartAwsBackupJob",
        "dynamodb:ListTagsOfResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "BackupGatewayBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Backup",
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
    },
    {
      "Sid" : "RedshiftCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterSnapshot",
```

```
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateSnapshot"
      ],
```

```
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*",
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsBackupJob",
        "timestream:GetAwsBackupStatus",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListTagsForResource",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPResourcePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLResourcePermissionsForBackup",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDSQLPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBackupAccessEntry",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "AssociateBackupAccessPolicy",
      "Effect" : "Allow",
```

```
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForBackup",
          "eks:accessScope" : "cluster"
        }
      }
    },
    {
      "Sid" : "GuardDutyMalwareScanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:StartMalwareScan",
        "guardduty:GetMalwareScan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyMalwareScanIAMPassPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupServiceRolePolicyForIndexing

Descrizione: Policy contenente le autorizzazioni necessarie per il AWS Backup per indicizzare i punti di ripristino.

`AWSBackupServiceRolePolicyForIndexing`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBackupServiceRolePolicyForIndexing` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 dicembre 2024, 18:37 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "KMSDataKeyForEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupServiceRolePolicyForItemRestores

Descrizione: Policy contenente le autorizzazioni necessarie per consentire a AWS Backup di ripristinare singoli elementi in un punto di ripristino

`AWSBackupServiceRolePolicyForItemRestores`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBackupServiceRolePolicyForItemRestores` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 dicembre 2024, 18:37 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "S3ReadonlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForFileLevelRestore",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "KMSDataKeyForS3AndEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupServiceRolePolicyForRestores

Descrizione: Fornisce l'autorizzazione AWS di Backup per eseguire ripristini per conto dell'utente su tutti AWS i servizi. Questa politica include le autorizzazioni per creare ed eliminare AWS risorse, come volumi EBS, istanze RDS e file system EFS, che fanno parte del processo di ripristino.

`AWSBackupServiceRolePolicyForRestores`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSBackupServiceRolePolicyForRestores` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 gennaio 2019, 00:23 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Versione della politica

Versione della politica: v35 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DeleteVolume",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:AddTagsToResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:CreateStorediSCSIVolume",
        "storagegateway:CreateCachediSCSIVolume"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "RDSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:DeleteDBInstance",
        "rds:AddTagsToResource",
```

```
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:DeleteDBCluster",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterToPointInTime",
        "rds:CreateTenantDatabase",
        "rds:DeleteTenantDatabase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Restore",
        "elasticfilesystem:CreateFilesystem",
        "elasticfilesystem:DescribeFilesystems",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLResourcePermissionsForRestore",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:TagResource",
        "dsql:CreateCluster",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:UpdateCluster",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetCluster"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "elasticfilesystem.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "dsql.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "EBSSnapshotBlockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:CompleteSnapshot",
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "RDSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "EC2DeleteAndRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:RestoreSnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsScopedPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "EC2RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TerminateInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateVolume"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystemFromBackup"
```

```
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
      "Sid" : "FsxTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteFileSystem",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "FsxDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
```

```
      "Sid" : "FsxVolumeTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "FsxBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "DSPermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromAwsBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "GatewayRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Restore"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "CloudformationChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:*/*/*"
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:RestoreFromClusterSnapshot",
        "redshift:RestoreTableFromClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
```

```
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeTableRestoreStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:RestoreTableFromSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessTablePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-serverless:GetTableRestoreStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsRestoreJob",
        "timestream:GetAwsRestoreStatus",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:ListDatabases",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EKSClusterRestore",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCluster",
        "eks:DescribeCluster",
        "eks:CreateAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:AssociateAccessPolicy",
        "eks:ListAssociatedAccessPolicies",
        "eks:CreateAddon",
```

```
        "eks:DescribeAddon",
        "eks:CreateNodegroup",
        "eks:DescribeNodegroup",
        "eks:CreateFargateProfile",
        "eks:DescribeFargateProfile",
        "eks:CreatePodIdentityAssociation",
        "eks:DescribePodIdentityAssociation",
        "eks:TagResource"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:access-entry/*",
        "arn:aws:eks:*:*:addon/*",
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:fargateprofile/*",
        "arn:aws:eks:*:*:nodegroup/*",
        "arn:aws:eks:*:*:podidentityassociation/*"
      ]
    },
    {
      "Sid" : "AssociateRestoreAccessPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForRestore",
          "eks:accessScope" : "cluster"
        }
      }
    },
    {
      "Sid" : "CreateClusterIAMPerms",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "eks.amazonaws.com",
            "ec2.amazonaws.com",
            "pods.eks.amazonaws.com",
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEKSNodeGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets",
        "ec2:RunInstances",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSNodeGroupTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "BackupRestoreJobManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:StartRestoreJob",
```

```
        "backup:ListRestoreJobs",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:DescribeRestoreJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupServiceRolePolicyForS3Backup

Descrizione: policy contenente le autorizzazioni necessarie per il AWS Backup per il backup dei dati in qualsiasi bucket S3. Ciò include l'accesso in lettura a tutti gli oggetti S3 e qualsiasi accesso di decrittografia per tutte le chiavi KMS.

`AWSBackupServiceRolePolicyForS3Backup`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSBackupServiceRolePolicyForS3Backup` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 febbraio 2022, 17:40 UTC
- Ora modificata: 17 maggio 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchGetMetricDataPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgePermissionsForAwsBackupManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeListRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:GetInventoryConfiguration",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutInventoryConfiguration",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/*"
    },
    {
```

```
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListAllMyBuckets",
      "Resource" : "*"
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupServiceRolePolicyForS3Restore

Descrizione: policy contenente le autorizzazioni necessarie per consentire a AWS Backup di ripristinare un backup S3 in un bucket. Ciò include read/write le autorizzazioni per tutti i bucket S3 e le autorizzazioni per e per tutte le chiavi KMS. GenerateDataKey DescribeKey

`AWSBackupServiceRolePolicyForS3Restore`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSBackupServiceRolePolicyForS3Restore` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 febbraio 2022, 17:39 UTC
- Ora modificata: 07 febbraio 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:PutBucketVersioning",
        "s3:PutBucketOwnershipControls",
        "s3:GetBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectVersionAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging",
        "s3:GetObjectAcl",
        "s3:PutObjectAcl",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBackupServiceRolePolicyForScans

Descrizione: Fornisce l'autorizzazione AWS di Backup per eseguire scansioni antimalware sui punti di AWS backup e ripristino

`AWSBackupServiceRolePolicyForScans`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBackupServiceRolePolicyForScans` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2025, 03:34 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForScans`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyMalwareScanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:StartMalwareScan",
        "guardduty:GetMalwareScan"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "IAMPassPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBatchFullAccess

Descrizione: Fornisce l'accesso completo alle risorse AWS Batch.

`AWSBatchFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBatchFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 dicembre 2016, 19:35 UTC
- Ora modificata: 24 ottobre 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:*",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeClusters",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:ListClusters",
        "logs:Describe*",
        "logs:Get*",
        "logs:TestMetricFilter",
```

```
        "logs:FilterLogEvents",
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/service-role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/ecsInstanceRole",
        "arn:aws:iam::*:instance-profile/ecsInstanceRole",
        "arn:aws:iam::*:role/iaws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/AWSBatchJobRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*Batch*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "batch.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBatchServiceEventTargetRole

Descrizione: politica per abilitare CloudWatch Event Target per l'invio di AWS Batch Job

`AWSBatchServiceEventTargetRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBatchServiceEventTargetRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 28 febbraio 2018, 22:31 UTC
- Ora modificata: 28 febbraio 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:SubmitJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBatchServiceRole

Descrizione: ruolo del servizio Policy for AWS Batch che consente l'accesso a servizi correlati tra cui EC2, Autoscaling, il servizio EC2 Container e Cloudwatch Logs.

`AWSBatchServiceRole`è una AWS policy gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBatchServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 dicembre 2016, 19:36 UTC
- Ora modificata: 05 dicembre 2023, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:TerminateInstances",
        "ec2:RunInstances",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "ecs:DescribeClusters",
```

```
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListAccountSettings",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeregisterTaskDefinition",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:UpdateContainerAgent",
        "ecs:DeregisterContainerInstance",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : [
        "arn:aws:ecs:*:*:task/*_Batch_*"
      ]
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBatchServiceRolePolicyForSageMaker

Descrizione: Fornisce l'accesso a AWS Batch per mettere in coda e gestire i carichi di lavoro Amazon SageMaker

`AWSBatchServiceRolePolicyForSageMaker`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 luglio 2025, 21:37 UTC
- Ora modificata: 16 aprile 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBatchServiceRolePolicyForSageMaker`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:ListTags",
        "sagemaker:DeleteTrainingJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateTrainingJob"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:Search"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBCMDataExportsServiceRolePolicy

Descrizione: un ruolo collegato al servizio per fornire ai dati di Billing and Cost Management Exports l'accesso AWS ai dati del servizio per esportare i dati in una posizione di destinazione, come Amazon S3, per conto di un cliente.

`AWSBCMDataExportsServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 giugno 2024, 17:40 UTC

- Ora modificata: 10 giugno 2024, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy

Descrizione: consente a Bedrock AgentCore Gateway di gestire le risorse VPC Lattice per tuo conto

`AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 28 marzo 2026, 22:12 UTC
- Ora modificata: 28 marzo 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSLRActionsForLattice",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway",
        "vpc-lattice:TagResource"
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:resourcegateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/BedrockAgentCoreGatewayManaged" : "true",
          "aws:ResourceTag/BedrockAgentCoreGatewayManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowEC2PermissionsForResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowResourceGatewayDelete",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeleteResourceGateway",
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/BedrockAgentCoreGatewayManaged" : "true"
```

```
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy

Descrizione: consente a Bedrock AgentCore Identity di gestire le risorse VPC Lattice per tuo conto

`AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 aprile 2026, 00:42 UTC
- Ora modificata: 15 aprile 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSLRActionsForLattice",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway",
        "vpc-lattice:TagResource"
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:resourcegateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/BedrockAgentCoreIdentityManaged" : "true",
          "aws:ResourceTag/BedrockAgentCoreIdentityManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowEC2PermissionsForResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowResourceGatewayDelete",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeleteResourceGateway",
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/BedrockAgentCoreIdentityManaged" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBillingConductorFullAccess

Descrizione: utilizza la policy AWSBilling ConductorFullAccess gestita per consentire l'accesso completo alla console AWS Billing Conductor (ABC) e APIs. Questa politica consente agli utenti di elencare, creare ed eliminare risorse ABC.

`AWSBillingConductorFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBillingConductorFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 aprile 2022, 18:02 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeResponsibilityTransfer",
        "organizations:ListInboundResponsibilityTransfers"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBillingConductorReadOnlyAccess

Descrizione: utilizza la policy AWSBilling ConductorReadOnlyAccess gestita per consentire l'accesso in sola lettura alla console AWS Billing Conductor (ABC) e APIs. Questa politica concede l'autorizzazione a visualizzare ed elencare tutte le risorse ABC. Non include la possibilità di creare o eliminare risorse.

`AWSBillingConductorReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBillingConductorReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 aprile 2022, 18:02 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "billingconductor:GetBillingGroupCostReport",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBillingReadOnlyAccess

Descrizione: consente agli utenti di visualizzare le fatture sulla Billing Console.

`AWSBillingReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBillingReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 agosto 2020, 20:08 UTC
- Ora modificata: 30 luglio 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Versione della politica

Versione della politica: v28 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetCredits",
        "billing:GetContractInformation",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "budgets:ViewBudget",
```

```
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostCategoryDefinitions",
        "ce:ListCostCategoryResourceAssociations",
        "ce:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostComparisonDrivers",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountPlanState",
        "freetier:GetAccountActivity",
        "freetier:ListAccountActivities",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "invoicing:ListProcurementPortals",
        "invoicing:ListProcurementPortalSuppliers",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
```

```
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBillingServiceRolePolicy

Descrizione: consente al servizio di fatturazione di convalidare l'accesso ai dati di visualizzazione della fatturazione per le visualizzazioni di fatturazione derivate

`AWSBillingServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 11 settembre 2025, 16:19 UTC
- Ora modificata: 11 settembre 2025, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBillingServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetBillingViewData"
      ],
      "Resource" : "arn:aws:billing::*:billingview/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

Descrizione: questa politica fornisce le autorizzazioni per controllare AWS le risorse. Ad esempio, per avviare e arrestare le istanze EC2 o RDS eseguendo script AWS Systems Manager (SSM).

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 25 maggio 2022, 19:03 UTC
- Ora modificata: 07 aprile 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StartRdsInstance",
        "arn:aws:ssm:*:*:document/AWS-StopRdsInstance",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBudgetsActionsWithAWSResourceControlAccess

Descrizione: fornisce l'accesso completo a AWS Budgets Actions, incluso l'utilizzo di Budgets Actions per controllare lo stato delle risorse in esecuzione AWS tramite Console di gestione AWS

`AWSBudgetsActionsWithAWSResourceControlAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBudgetsActionsWithAWSResourceControlAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 ottobre 2020, 17:19 UTC
- Ora modificata: 15 ottobre 2020, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "budgets:*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ModifyBilling",
        "ec2:DescribeInstances",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListPolicies",
        "organizations:ListRoots",
        "rds:DescribeDBInstances",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBudgetsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS Budgets Console tramite. Console di gestione AWS

`AWSBudgetsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBudgetsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 ottobre 2020, 17:18 UTC
- Ora modificata: 17 giugno 2024, 17:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBudgetsSpendLimitMemberRolePolicy

Descrizione: concede al servizio AWS Budgets le autorizzazioni per descrivere, interrompere e terminare le risorse di un account membro per far rispettare le azioni relative ai limiti di spesa.

`AWSBudgetsSpendLimitMemberRolePolicy`è una politica gestita. AWS

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 18 luglio 2026, 00:57 UTC
- Ora modificata: 18 luglio 2026, 00:57 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBudgetsSpendLimitMemberRolePolicy`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:StopInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeAddresses",
        "ec2:DescribeSnapshots",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSActions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:StopDBInstance",
        "rds:DescribeDBClusters",
        "rds:StopDBCluster",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
```

```
        "rds:DescribeIntegrations",
        "rds:DescribeDBProxies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLActions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:ListNotebookInstances",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListTrainingJobs",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:ListProcessingJobs",
        "sagemaker:StopProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:StopTransformJob",
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:DescribeCluster",
        "sagemaker:ListClusters",
        "sagemaker:DescribeClusterNode",
        "sagemaker:ListClusterNodes",
        "sagemaker:AttachClusterNodeVolume",
        "sagemaker:DetachClusterNodeVolume",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:ListMlflowTrackingServers",
```

```
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:StopLabelingJob",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaActions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:GetFunctionConcurrency",
        "lambda:PutFunctionConcurrency",
        "lambda:DeleteFunctionConcurrency",
        "lambda:ListEventSourceMappings",
        "lambda:GetEventSourceMapping",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockActions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:UpdateProvisionedModelThroughput",
        "bedrock:GetModelInvocationJob",
        "bedrock:ListModelInvocationJobs",
        "bedrock:StopModelInvocationJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:StopModelCustomizationJob",
        "bedrock:GetEvaluationJob",
        "bedrock:ListEvaluationJobs",
        "bedrock:StopEvaluationJob"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StartRdsInstance",
        "arn:aws:ssm:*:*:document/AWS-StopRdsInstance",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
      ]
    },
    {
      "Sid" : "ComputeOptimizerActions",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetIdleRecommendations",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEnrollmentStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeOptimizerAutomationActions",
      "Effect" : "Allow",
      "Action" : [
        "aco-automation:StartAutomationEvent",
        "aco-automation:ListRecommendedActions",
        "aco-automation:GetAutomationEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sso:ListInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccountActions",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetPrimaryEmail"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBugBustFullAccess

Descrizione: questa policy IAM garantisce agli utenti l'accesso completo alla console AWS BugBust

`AWSBugBustFullAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBugBustFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2021, 07:03 UTC
- Ora modificata: 22 luglio 2021, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustSLRCreation",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/bugbust.amazonaws.com/
AWSServiceRoleForBugBust",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "bugbust.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBugBustPlayerAccess

Descrizione: questa policy IAM consente agli utenti di accedere alla partecipazione AWS BugBust agli eventi

`AWSBugBustPlayerAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSBugBustPlayerAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2021, 07:15 UTC
- Ora modificata: 24 giugno 2021, 07:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustPlayerAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:ListBugs",
        "bugbust:ListProfilingGroups",
        "bugbust:JoinEvent",
        "bugbust:GetEvent",
        "bugbust:ListEvents",
        "bugbust:GetJoinEventStatus",
        "bugbust:ListEventScores",
        "bugbust:ListEventParticipants",
        "bugbust:UpdateWorkItem",
```

```
        "bugbust:ListPullRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSBugBustServiceRolePolicy

Descrizione: concede le autorizzazioni per accedere AWS BugBust alle risorse per tuo conto

`AWSBugBustServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 24 giugno 2021, 06:59 UTC
- Ora modificata: 24 giugno 2021, 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCertificateManagerFullAccess

Descrizione: Fornisce l'accesso completo a AWS Certificate Manager (ACM)

`AWSCertificateManagerFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCertificateManagerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 gennaio 2016, 17:02 UTC
- Ora modificata: 17 agosto 2020, 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "acm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCertificateManagerPrivateCAAuditor

Descrizione: Fornisce l'accesso dei revisori all'autorità di certificazione privata di AWS Certificate Manager

`AWSCertificateManagerPrivateCAAuditor`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCertificateManagerPrivateCAAuditor` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 ottobre 2018, 16:51 UTC
- Ora modificata: 17 agosto 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCertificateManagerPrivateCAFullAccess

Descrizione: Fornisce l'accesso completo all'autorità di AWS certificazione privata di Certificate Manager

`AWSCertificateManagerPrivateCAFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCertificateManagerPrivateCAFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 ottobre 2018, 16:54 UTC
- Ora modificata: 23 ottobre 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCertificateManagerPrivateCAPrivilegedUser

Descrizione: fornisce agli utenti dei certificati l'accesso privilegiato all'autorità di certificazione privata di AWS Certificate Manager

`AWSCertificateManagerPrivateCAPrivilegedUser`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCertificateManagerPrivateCAPrivilegedUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 giugno 2019, 17:43 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
```

```
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCertificateManagerPrivateCAReadOnly

Descrizione: fornisce l'accesso in sola lettura all'autorità di AWS certificazione privata di Certificate Manager

`AWSCertificateManagerPrivateCAReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCertificateManagerPrivateCAReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 ottobre 2018, 16:57 UTC
- Ora modificata: 17 agosto 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCertificateManagerPrivateCAUser

Descrizione: Fornisce agli utenti del certificato l'accesso all'autorità di AWS certificazione privata di Certificate Manager

`AWSCertificateManagerPrivateCAUser`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCertificateManagerPrivateCAUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 ottobre 2018, 16:53 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
```

```
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCertificateManagerReadOnly

Descrizione: fornisce l'accesso in sola lettura a AWS Certificate Manager (ACM).

`AWSCertificateManagerReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCertificateManagerReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 gennaio 2016, 17:07 UTC
- Ora modificata: 30 giugno 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:SearchCertificates",
```

```
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration",
      "acm:DescribeAcmeAccount",
      "acm:DescribeAcmeDomainValidation",
      "acm:DescribeAcmeEndpoint",
      "acm:DescribeAcmeExternalAccountBinding",
      "acm:ListAcmeAccounts",
      "acm:ListAcmeDomainValidations",
      "acm:ListAcmeEndpoints",
      "acm:ListAcmeExternalAccountBindings",
      "acm:ListTagsForResource"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSChatbotServiceLinkedRolePolicy

Descrizione: il ruolo collegato al servizio utilizzato dal AWS Chatbot.

`AWSChatbotServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 novembre 2019, 16:39 UTC

- Ora modificata: 18 novembre 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Unsubscribe",
        "sns:Subscribe",
        "sns:ListSubscriptions"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/chatbot/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCleanRoomsFullAccess

Descrizione: consente l'accesso completo alle risorse di AWS Clean Rooms e l'accesso alle risorse correlate Servizi AWS.

`AWSCleanRoomsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCleanRoomsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2023, 16:10 UTC
- Ora modificata: 21 marzo 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickQueryResultsBucketListAll",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SetQueryResultsBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
```

```
      "Sid" : "WriteQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleDisplayQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCleanRoomsFullAccessNoQuerying

Descrizione: consente l'accesso completo alle risorse di AWS Clean Rooms ad eccezione delle interrogazioni in collaborazione e dell'accesso alle risorse correlate Servizi AWS.

`AWSCleanRoomsFullAccessNoQuerying`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCleanRoomsFullAccessNoQuerying` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2023, 16:12 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
```

```
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableReference",
        "cleanrooms:UpdateConfiguredTableAllowedColumns",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsNoQuerying",
      "Effect" : "Deny",
      "Action" : [
        "cleanrooms:StartProtectedQuery",
        "cleanrooms:UpdateProtectedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
```

```
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCleanRoomsMLFullAccess

Descrizione: consente l'accesso completo alle risorse AWS Clean Rooms ML e l'accesso alle relative Servizi AWS.

`AWSCleanRoomsMLFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCleanRoomsMLFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2023, 21:02 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CollaborationMembershipCheck",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:ListMembers"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cleanrooms-ml.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AssociateModels",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:CreateConfiguredAudienceModelAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAssociations",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:TagResource"
      ],
      "Resource" : "arn:aws:cleanrooms:*:*:membership/*/
configuredaudiencemodelassociation/*"
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cleanrooms-ml*",
        "arn:aws:iam::*:role/role/cleanrooms-ml*"
      ]
```

```
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanroomsml*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickOutputBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickS3Location",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*cleanrooms-ml*"
    },
    {
      "Sid" : "ConsoleDescribeECRRepositories",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:ListImages"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCleanRoomsMLReadOnlyAccess

Descrizione: consente l'accesso in sola lettura alle risorse AWS Clean Rooms ML e l'accesso in sola lettura alle risorse Clean Rooms correlate AWS

`AWSCleanRoomsMLReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSCleanRoomsMLReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2023, 20:55 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
```

```
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsMLRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCleanRoomsReadOnlyAccess

Descrizione: consente l'accesso in sola lettura alle risorse AWS Clean Rooms e l'accesso in sola lettura alle risorse AWS Glue e Amazon Logs correlate. CloudWatch

`AWSCleanRoomsReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSCleanRoomsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 gennaio 2023, 16:10 UTC
- Ora modificata: 12 gennaio 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGet*",
        "cleanrooms:Get*",
        "cleanrooms:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCleanRoomsServiceRolePolicy

Descrizione: consenti a AWS Clean Rooms di accedere ad altri AWS servizi, ad esempio per tuo CloudWatch APIs conto.

`AWSCleanRoomsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 dicembre 2025, 17:49 UTC
- Ora modificata: 15 dicembre 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCleanRoomsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Clean Rooms"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloud9Administrator

Descrizione: fornisce l'accesso come amministratore a AWS Cloud9.

`AWSCloud9Administrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloud9Administrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:17 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:*",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
```

```
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloud9EnvironmentMember

Descrizione: offre la possibilità di essere invitato negli ambienti di sviluppo AWS condivisi Cloud9.

`AWSCloud9EnvironmentMember`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloud9EnvironmentMember` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:18 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserSettings",
        "cloud9:UpdateUserSettings",
        "cloud9:GetMigrationExperiences",
        "iam:GetUser",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloud9ServiceRolePolicy

Descrizione: policy Service Linked Role per AWS Cloud9

`AWSCloud9ServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 30 novembre 2017, 13:44 UTC
- Ora modificata: 17 gennaio 2022, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-cloud9-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/cloud9/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSCloud9SSMAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloud9SSMInstanceProfile

Descrizione: questa policy verrà utilizzata per assegnare un ruolo a Cloud9 di utilizzare SSM Session Manager per connettersi all'istanza InstanceProfile

`AWSCloud9SSMInstanceProfile`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSCloud9SSMInstanceProfile` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 maggio 2020, 11:40 UTC
- Ora modificata: 14 maggio 2020, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloud9User

Descrizione: Fornisce l'autorizzazione per creare AWS ambienti di sviluppo Cloud9 e gestire ambienti di proprietà.

`AWSCloud9User`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloud9User` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2017, 16:16 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "cloud9:GetMigrationExperiences",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:CreateEnvironmentEC2",
        "cloud9:CreateEnvironmentSSH"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:OwnerArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudFormationFullAccess

Descrizione: Fornisce accesso completo a AWS CloudFormation.

`AWSCloudFormationFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudFormationFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 luglio 2019, 21:50 UTC
- Ora modificata: 26 luglio 2019, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudFormationReadOnlyAccess

Descrizione: Fornisce l'accesso AWS CloudFormation tramite Console di gestione AWS.

`AWSCloudFormationReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudFormationReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:BatchDescribe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudFrontLogger

Descrizione: concede a CloudFront Logger i permessi di scrittura per Logs. CloudWatch

`AWSCloudFrontLogger`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 giugno 2018, 20:15 UTC
- Ora modificata: 22 novembre 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudFrontVPCOriginServiceRolePolicy

Descrizione: consente di CloudFront gestire le interfacce di rete elastiche e i gruppi di sicurezza EC2 per tuo conto.

`AWSCloudFrontVPCOriginServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 24 ottobre 2024, 17:45 UTC
- Ora modificata: 24 ottobre 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontVPCOriginServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "EC2Action5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled",
          "ec2:CreateAction" : [
```

```
            "CreateNetworkInterface",
            "CreateSecurityGroup"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudHSMFullAccess

Descrizione: fornisce l'accesso completo a tutte le risorse CloudHSM.

`AWSCloudHSMFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudHSMFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 6 febbraio 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudhsm:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudHSMReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a tutte le risorse CloudHSM.

`AWSCloudHSMReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudHSMReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 6 febbraio 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Get*",
        "cloudhsm:List*",
        "cloudhsm:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudHSMRole

Descrizione: policy predefinita per il ruolo del servizio AWS CloudHSM.

`AWSCloudHSMRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudHSMRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudMapDiscoverInstanceAccess

Descrizione: fornisce l'accesso all'API Cloud AWS Map Discovery.

`AWSCloudMapDiscoverInstanceAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudMapDiscoverInstanceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2018, 00:02 UTC
- Ora modificata: 20 settembre 2023, 21:48 UTC

- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudMapFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni della Cloud AWS mappa.

`AWSCloudMapFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudMapFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 23:57 UTC
- Ora modificata: 29 luglio 2020, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
```

```
        "ec2:DescribeInstances",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudMapReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutte le azioni della Cloud AWS mappa.

`AWSCloudMapReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudMapReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 23:45 UTC
- Ora modificata: 20 settembre 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudMapRegisterInstanceAccess

Descrizione: fornisce l'accesso a livello di registrante alle azioni della Cloud AWS mappa.

`AWSCloudMapRegisterInstanceAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudMapRegisterInstanceAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2018, 00:04 UTC
- Ora modificata: 20 settembre 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudShellFullAccess

Descrizione: concede l'utilizzo AWS CloudShell con tutte le funzionalità

`AWSCloudShellFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudShellFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 18:07 UTC
- Ora modificata: 15 dicembre 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudshell:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudTrail_FullAccess

Descrizione: fornisce accesso completo a AWS CloudTrail.

`AWSCloudTrail_FullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudTrail_FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 ottobre 2020, 23:41 UTC
- Ora modificata: 22 febbraio 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-cloudtrail-logs*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudtrail:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudtrail.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudTrail_ReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a AWS CloudTrail.

`AWSCloudTrail_ReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCloudTrail_ReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 14 giugno 2022, 17:19 UTC
- Ora modificata: 14 giugno 2022, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:Get*",
        "cloudtrail:Describe*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

Descrizione: questo criterio viene utilizzato dal ruolo collegato al servizio denominato. AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents CloudWatch utilizza questo ruolo collegato al servizio per eseguire azioni di AWS System Manager Incident Manager quando un CloudWatch allarme entra nello stato ALARM. Questa politica concede il permesso di avviare incidenti per conto dell'utente.

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 27 aprile 2021, 13:30 UTC
- Ora modificata: 27 aprile 2021, 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeArtifactAdminAccess

Descrizione: Fornisce l'accesso completo AWS CodeArtifact tramite Console di gestione AWS.

`AWSCodeArtifactAdminAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeArtifactAdminAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 giugno 2020, 23:53 UTC
- Ora modificata: 16 giugno 2020, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeArtifactReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura AWS CodeArtifact tramite Console di gestione AWS.

`AWSCodeArtifactReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeArtifactReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 giugno 2020, 21:23 UTC
- Ora modificata: 25 giugno 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:Describe*",
        "codeartifact:Get*",
        "codeartifact:List*",
        "codeartifact:ReadFromRepository"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeBuildAdminAccess

Descrizione: Fornisce l'accesso completo AWS CodeBuild tramite Console di gestione AWS. Collega anche AmazonS3 ReadOnlyAccess per fornire l'accesso al download degli artefatti della build e collega IAMFull Access per creare e gestire il ruolo di servizio per. CodeBuild

`AWSCodeBuildAdminAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSCodeBuildAdminAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2016, 19:04 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Versione della politica

Versione della politica: v20 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "SSMOpenDataChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "CodeStarConnectionsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:UpdateConnectionInstallation",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListConnections",
```

```
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:ListTagsForResource",
        "codestar-connections:GetConnection",
        "codestar-connections:GetIndividualAccessToken",
        "codestar-connections:GetInstallationUrl",
        "codestar-connections:PassConnection",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeBuildDeveloperAccess

Descrizione: fornisce l'accesso AWS CodeBuild tramite Console di gestione AWS, ma non consente l'amministrazione CodeBuild del progetto. Inoltre, collega AmazonS3 ReadOnlyAccess per consentire l'accesso al download degli artefatti della build.

`AWSCodeBuildDeveloperAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSCodeBuildDeveloperAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2016, 19:02 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Versione della politica

Versione della politica: v21 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
```

```
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "SSMOpenDataChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
```

```
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeBuildReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura AWS CodeBuild tramite Console di gestione AWS. Inoltre, collega AmazonS3 ReadOnlyAccess per consentire l'accesso al download degli artefatti della build.

`AWSCodeBuildReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSCodeBuildReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2016, 19:03 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeCommitFullAccess

Descrizione: Fornisce l'accesso completo AWS CodeCommit tramite Console di gestione AWS.

`AWSCodeCommitFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeCommitFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:02 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
```

```
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
```

```
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeCommitPowerUser

Descrizione: fornisce l'accesso completo ai AWS CodeCommit repository, ma non consente l'eliminazione degli archivi.

`AWSCodeCommitPowerUser`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeCommitPowerUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:06 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Versione della politica

Versione della politica: v18 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
```

```
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeCommitReadOnly

Descrizione: fornisce l'accesso in sola lettura AWS CodeCommit tramite Console di gestione AWS.

`AWSCodeCommitReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeCommitReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:05 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials",
        "iam:ListAccessKeys",
        "iam:GetSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeDeployDeployerAccess

Descrizione: fornisce l'accesso per registrare e distribuire una revisione.

`AWSCodeDeployDeployerAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeDeployDeployerAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 maggio 2015, 18:18 UTC

- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
```

```
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeDeployFullAccess

Descrizione: fornisce l'accesso completo alle CodeDeploy risorse.

`AWSCodeDeployFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeDeployFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 maggio 2015, 18:13 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "codedeploy:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
```

```
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeDeployReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle CodeDeploy risorse.

`AWSCodeDeployReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeDeployReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 maggio 2015, 18:21 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeDeployRole

Descrizione: Fornisce l'accesso al CodeDeploy servizio per espandere i tag e interagire con Auto Scaling per tuo conto.

`AWSCodeDeployRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeDeployRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 4 maggio 2015, 18:05 UTC
- Ora modificata: 16 agosto 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:PutLifecycleHook",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:SuspendProcesses",
        "autoscaling:ResumeProcesses",
        "autoscaling:AttachLoadBalancers",
        "autoscaling:AttachLoadBalancerTargetGroups",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutWarmPool",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DeleteAutoScalingGroup",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:TerminateInstances",
        "tag:GetResources",
        "sns:Publish",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
```

```
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeDeployRoleForCloudFormation

Descrizione: fornisce l'accesso al CodeDeploy servizio per richiamare la funzione Lambda per conto dell'utente per blue/green eseguire la distribuzione. CloudFormation

`AWSCodeDeployRoleForCloudFormation`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeDeployRoleForCloudFormation` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 maggio 2020, 17:12 UTC
- Ora modificata: 19 maggio 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeDeployRoleForECS

Descrizione: fornisce l'accesso a livello di CodeDeploy servizio per eseguire un' blue/green implementazione ECS per tuo conto. Garantisce l'accesso completo ai servizi di supporto, come l'accesso completo per leggere tutti gli oggetti S3, richiamare tutte le funzioni Lambda, pubblicare su tutti gli argomenti SNS all'interno dell'account e aggiornare tutti i servizi ECS.

`AWSCodeDeployRoleForECS`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSCodeDeployRoleForECS` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 20:40 UTC
- Ora modificata: 23 settembre 2019, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule",
        "lambda:InvokeFunction",
        "cloudwatch:DescribeAlarms",
        "sns:Publish",
        "s3:GetObject",
```

```
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeDeployRoleForECSLimited

Descrizione: fornisce un accesso limitato al CodeDeploy servizio per eseguire un' blue/green implementazione ECS per tuo conto.

`AWSCodeDeployRoleForECSLimited`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeDeployRoleForECSLimited` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 20:42 UTC
- Ora modificata: 23 settembre 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeDeployTopic_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
```

```
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsTaskExecutionRole",
        "arn:aws:iam::*:role/ECSTaskExecution*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeDeployRoleForLambda

Descrizione: fornisce l'accesso al CodeDeploy servizio per eseguire una distribuzione Lambda per tuo conto.

`AWSCodeDeployRoleForLambda`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeDeployRoleForLambda` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 28 novembre 2017, 14:05 UTC
- Ora modificata: 03 dicembre 2019, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig",
        "sns:Publish"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeDeployRoleForLambdaLimited

Descrizione: fornisce un accesso limitato al CodeDeploy servizio per eseguire una distribuzione Lambda per tuo conto.

`AWSCodeDeployRoleForLambdaLimited`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeDeployRoleForLambdaLimited` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 agosto 2020, 17:14 UTC
- Ora modificata: 17 agosto 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodePipeline_FullAccess

Descrizione: Fornisce l'accesso completo AWS CodePipeline tramite Console di gestione AWS.

`AWSCodePipeline_FullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodePipeline_FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 agosto 2020, 22:38 UTC
- Ora modificata: 14 marzo 2024, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListChangeSets",
        "cloudtrail:DescribeTrails",
        "codebuild:BatchGetProjects",
        "codebuild:CreateProject",
        "codebuild:ListCuratedEnvironmentImages",
        "codebuild:ListProjects",
        "codecommit:ListBranches",
        "codecommit:GetReferences",
        "codecommit:ListRepositories",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:ListClusters",
        "ecs:ListServices",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "iam:ListRoles",
        "iam:GetRole",
        "lambda:ListFunctions",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:DescribeRule",
        "opsworks:DescribeApps",
        "opsworks:DescribeLayers",
        "opsworks:DescribeStacks",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
```

```
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes",
        "states:ListStateMachines"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "CodePipelineAuthoringAccess"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetObjectVersion",
        "s3:CreateBucket",
        "s3:PutBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*",
      "Sid" : "CodePipelineArtifactsReadWriteAccess"
    },
    {
      "Action" : [
        "cloudtrail:PutEventSelectors",
        "cloudtrail:CreateTrail",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:StartLogging"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudtrail:*:*:trail/codepipeline-source-trail",
      "Sid" : "CodePipelineSourceTrailReadWriteAccess"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cwe-role-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "events.amazonaws.com"
          ]
        }
      },
      "Sid" : "EventsIAMPassRole"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codepipeline.amazonaws.com"
          ]
        }
      },
      "Sid" : "CodePipelineIAMPassRole"
    },
    {
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:DisableRule",
        "events:RemoveTargets"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:events:*:*:rule/codepipeline-*"
      ],
      "Sid" : "CodePipelineEventsReadWriteAccess"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
```

```
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodePipeline_ReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura AWS CodePipeline tramite Console di gestione AWS.

`AWSCodePipeline_ReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodePipeline_ReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 agosto 2020, 22:25 UTC
- Ora modificata: 03 agosto 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListActionExecutions",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodePipelineApproverAccess

Descrizione: fornisce l'accesso per visualizzare e approvare le modifiche manuali per tutte le pipeline

`AWSCodePipelineApproverAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodePipelineApproverAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 luglio 2016, 18:59 UTC
- Ora modificata: 02 agosto 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodePipelineCustomActionAccess

Descrizione: fornisce l'accesso ad azioni personalizzate per verificare i dettagli delle offerte di lavoro (incluse le credenziali temporanee) e segnalare gli aggiornamenti di stato. AWS CodePipeline

`AWSCodePipelineCustomActionAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodePipelineCustomActionAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:02 UTC
- Ora modificata: 9 luglio 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
```

```
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeStarFullAccess

Descrizione: Fornisce l'accesso completo AWS CodeStar tramite Console di gestione AWS.

`AWSCodeStarFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeStarFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 aprile 2017, 16:23 UTC
- Ora modificata: 28 marzo 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeStarEC2",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "cloud9:DescribeEnvironment*",
        "cloud9:ValidateEnvironmentName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarCF",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:ListStacks*",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeStarNotificationsServiceRolePolicy

Descrizione: consente alle AWS CodeStar notifiche di accedere ad Amazon CloudWatch Events per tuo conto

`AWSCodeStarNotificationsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 5 novembre 2019, 16:10 UTC
- Ora modificata: 19 marzo 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/awscodestarnotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeStarNotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommentsForComparedCommit",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:UpdateSlackChannelConfiguration",
        "codecommit:GetDifferences",
        "codepipeline:ListActionExecutions"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "codecommit:GetFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/ExcludeFileContentFromNotifications" : "true"
        }
      },
```

```
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCodeStarServiceRole

Descrizione: DO NOT USE - AWS CodeStar Service Role Policy che concede privilegi amministrativi per CodeStar gestire IAM e altre risorse di servizio per conto del cliente.

`AWSCodeStarServiceRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCodeStarServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 aprile 2017, 15:20 UTC
- Ora modificata: 20 settembre 2021, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProjectEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:RemoveTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*Stack*",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*",
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
        "arn:aws:cloudformation:*:aws:transform/CodeStar*"
      ]
    },
    {
      "Sid" : "ProjectStackTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeChangeSet"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectQuickstarts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awscodestar-*/*"
      ]
    },
    {
      "Sid" : "ProjectS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-codestar-*",
        "arn:aws:s3:::elasticbeanstalk-*"
      ]
    },
    {
      "Sid" : "ProjectServices",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "codecommit:*",
        "codepipeline:*",
        "codedeploy:*",
        "codebuild:*",
        "autoscaling:*",
        "cloudwatch:Put*",
        "ec2:*",
        "elasticbeanstalk:*",
        "elasticloadbalancing:*",
        "iam:ListRoles",
        "logs:*",
        "sns:*",
        "cloud9:CreateEnvironmentEC2",
        "cloud9:DeleteEnvironment",
        "cloud9:DescribeEnvironment*",
        "cloud9:ListEnvironments"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectWorkerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRole",
        "iam:PassRole",
        "iam:GetRolePolicy",
        "iam:PutRolePolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CodeStarWorker*",
        "arn:aws:iam::*:policy/CodeStarWorker*",
        "arn:aws:iam::*:instance-profile/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectTeamMembers",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachUserPolicy",
        "iam:DetachUserPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::*:policy/CodeStar_*"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/CodeStar_*"
      ]
    },
    {
      "Sid" : "InspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-codestar-service-role",
        "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
      ]
    },
    {
      "Sid" : "IAMLinkRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "DescribeConfigRuleForARN",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ProjectCodeStarConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectCodeStarConnectionsPassConnections",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCompromisedKeyQuarantine

Descrizione: nega l'accesso a determinate azioni, applicate dal AWS team nel caso in cui le credenziali di un utente IAM siano state compromesse o esposte pubblicamente. NON rimuovere questa politica. Segui invece le istruzioni specificate nell'e-mail che ti è stata inviata in merito a questo evento.

`AWSCompromisedKeyQuarantine`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCompromisedKeyQuarantine` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 agosto 2020, 18:04 UTC
- Ora modificata: 11 agosto 2020, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachGroupPolicy",
```

```
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateUser",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "lambda:CreateFunction",
        "lightsail:Create*",
        "lightsail:Start*",
        "lightsail:Delete*",
        "lightsail:Update*",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:DownloadDefaultKeyPair"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCompromisedKeyQuarantineV2

Descrizione: nega l'accesso a determinate azioni, applicate dal AWS team nel caso in cui le credenziali di un utente IAM siano state compromesse o esposte pubblicamente. NON rimuovere questa politica. Segui invece le istruzioni specificate nella richiesta di assistenza creata per te in merito a questo evento.

`AWSCompromisedKeyQuarantineV2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCompromisedKeyQuarantineV2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 aprile 2021, 22:30 UTC
- Ora modificata: 2 ottobre 2024, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
```

```
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
```

```
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
        "bedrock:PutFoundationModelEntitlement",
        "bedrock:InvokeModel",
        "s3:CreateBucket",
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
        "iam:DeleteRole",
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:GetEventSourceMapping",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCompromisedKeyQuarantineV3

Descrizione: nega l'accesso a determinate azioni, applicate da AWS nel caso in cui le credenziali di un utente IAM siano state compromesse o esposte pubblicamente. La politica mira a limitare i potenziali danni che possono essere causati da attività legate alla frode che portano ad addebiti non autorizzati, senza influire sulle risorse esistenti. NON rimuovere questa politica. Segui invece le istruzioni specificate nella richiesta di assistenza creata per te in merito a questo evento.

`AWSCompromisedKeyQuarantineV3`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSCompromisedKeyQuarantineV3` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 agosto 2024, 17:36 UTC
- Ora modificata: 16 marzo 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV3`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "iam:DeleteRole",
```

```
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:GetEventSourceMapping",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "organizations:LeaveOrganization",
        "organizations:AcceptHandshake",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "s3:CreateBucket",
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutEncryptionConfiguration",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
```

```
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
        "bedrock:PutFoundationModelEntitlement",
        "bedrock:InvokeModel",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel",
        "logs:PutLogEvents",
        "kms:PutKeyPolicy",
        "kms:RetireGrant",
        "kms:RevokeGrant",
        "kms:ScheduleKeyDeletion",
        "kms:DeleteImportedKeyMaterial"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:ViaService" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSConfigMultiAccountSetupPolicy

Descrizione: consente a Config di chiamare AWS i servizi e distribuire risorse di configurazione in tutta l'organizzazione

`AWSConfigMultiAccountSetupPolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 giugno 2019, 18:03 UTC
- Ora modificata: 24 febbraio 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Resource" : "arn:aws:config:*:*:conformance-pack/aws-service-conformance-pack/
config-multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSConfigRemediationServiceRolePolicy

Descrizione: consente a AWS Config di correggere le risorse non conformi per tuo conto.

`AWSConfigRemediationServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 giugno 2019, 21:21 UTC
- Ora modificata: 18 giugno 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
```

```
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      },
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSConfigRoleForOrganizations

Descrizione: consente a AWS Config di chiamare Organizzazioni di sola lettura AWS APIs

`AWSConfigRoleForOrganizations`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSConfigRoleForOrganizations` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 marzo 2018, 22:53 UTC
- Ora modificata: 24 novembre 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSConfigRulesExecutionRole

Descrizione: consente a una funzione AWS Lambda di accedere all'API AWS Config e agli snapshot di configurazione che Config AWS fornisce periodicamente ad Amazon S3. Questo accesso è richiesto dalle funzioni che valutano le modifiche alla configurazione per le regole di Config personalizzate.

`AWSConfigRulesExecutionRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSConfigRulesExecutionRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 25 marzo 2016, 17:59 UTC
- Ora modificata: 13 maggio 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSLogs/*/Config/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Put*",
        "config:Get*",
        "config:List*",
        "config:Describe*",
```

```
        "config:BatchGet*",
        "config:Select*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSConfigServiceRolePolicy

Descrizione: consente a Config di chiamare AWS i servizi e raccogliere le configurazioni delle risorse per conto dell'utente.

`AWSConfigServiceRolePolicy`è una policy AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 30 maggio 2018, 23:31 UTC
- Ora modificata: 30 luglio 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Versione della politica

Versione della politica: v94 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
```

```
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListVpcEndpoints",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
```

```
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListTagsForResource",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
```

```
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetApiAssociation",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListGraphqlApis",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
```

```
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetControl",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
```

```
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-dashboards:GetDashboard",
        "bcm-dashboards:ListDashboards",
        "bcm-dashboards:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyEngineSummary",
        "bedrock-agentcore:GetPolicySummary",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowsers",
```

```
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyEngineSummaries",
        "bedrock-agentcore:ListPolicySummaries",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
```

```
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "chime:DescribeAppInstance",
        "chime:ListAppInstances",
        "chime:ListTagsForResource",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
```

```
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
```

```
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListFunctions",
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListManagedInsightRules",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
```

```
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListFleets",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
```

```
        "cognito-idp:AdminGetUser",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeManagedLoginBranding",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeEmailAddress",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
```

```
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeView",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListEvaluationFormVersions",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUsers",
        "connect:ListViews",
        "connect:ListViewVersions",
        "connect:SearchAvailablePhoneNumbers",
        "controltower:GetLandingZone",
        "controltower:ListLandingZones",
        "cur:DescribeReportDefinitions",
```

```
        "cur:ListTagsForResource",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListPolicyGrants",
```

```
        "datazone:ListProjectMemberships",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetStorageProfile",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueues",
        "deadline:ListStorageProfiles",
        "deadline:ListTagsForResource",
        "detective:ListGraphs",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
```

```
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
```

```
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
```

```
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetAutoTerminationPolicy",
```

```
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
```

```
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
```

```
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerFleet",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScalingPolicies",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
```

```
        "gameliftstreams:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeAcceleratorAttributes",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
```

```
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetSession",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSessions",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:GetDeployment",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "greengrass:ListDeployments",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatEntitySet",
```

```
        "guardduty:GetThreatIntelSet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
```

```
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "internetmonitor:GetMonitor",
```

```
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackages",
        "iot:ListPackageVersions",
        "iot:ListPolicies",
```

```
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID2",
      "Effect" : "Allow",
      "Action" : [
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
```

```
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
```

```
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
```

```
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra-ranking:ListTagsForResource",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
```

```
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
```

```
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "license-manager:ListTagsForResource",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
```

```
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
```

```
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNode",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListNodes",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
```

```
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
```

```
        "mpa:GetIdentitySource",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "mq:ListTags",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "notifications:GetEventRule",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
```

```
        "notifications:ListTagsForResource",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListSinks",
        "oam:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:ListAnnotationStores",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
```

```
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:GetSite",
        "outposts:ListSites",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
```

```
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetPolicy",
        "qbusiness:ListApplications",
        "qbusiness:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "ram:GetPermission",
```

```
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
```

```
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListCollections",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
```

```
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
```

```
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rtbfabric:GetInboundExternalLink",
        "rtbfabric:GetLink",
        "rtbfabric:GetOutboundExternalLink",
        "rtbfabric:GetRequesterGateway",
        "rtbfabric:GetResponderGateway",
        "rtbfabric:ListLinks",
        "rtbfabric:ListRequesterGateways",
        "rtbfabric:ListResponderGateways",
        "rtbfabric:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
```

```
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
```

```
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:ListTableBuckets",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterSchedulerConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeContext",
```

```
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListActions",
```

```
            "sagemaker:ListAlgorithms",
            "sagemaker:ListAppImageConfigs",
            "sagemaker:ListApps",
            "sagemaker:ListArtifacts",
            "sagemaker:ListAutoMLJobs",
            "sagemaker:ListClusters",
            "sagemaker:ListClusterSchedulerConfigs",
            "sagemaker:ListCodeRepositories",
            "sagemaker:ListContexts",
            "sagemaker:ListDataQualityJobDefinitions",
            "sagemaker:ListDeviceFleets",
            "sagemaker:ListDomains",
            "sagemaker:ListEndpointConfigs",
            "sagemaker:ListEndpoints",
            "sagemaker:ListExperiments",
            "sagemaker:ListFeatureGroups",
            "sagemaker:ListFlowDefinitions",
            "sagemaker:ListHubs",
            "sagemaker:ListHumanTaskUis",
            "sagemaker:ListHyperParameterTuningJobs",
            "sagemaker:ListImages",
            "sagemaker:ListImageVersions",
            "sagemaker:ListInferenceComponents",
            "sagemaker:ListInferenceExperiments",
            "sagemaker:ListLabelingJobs",
            "sagemaker:ListMlflowApps",
            "sagemaker:ListMlflowTrackingServers",
            "sagemaker:ListModelBiasJobDefinitions",
            "sagemaker:ListModelCardExportJobs",
            "sagemaker:ListModelCards",
            "sagemaker:ListModelCardVersions",
            "sagemaker:ListModelExplainabilityJobDefinitions",
            "sagemaker:ListModelPackageGroups",
            "sagemaker:ListModelPackages",
            "sagemaker:ListModelQualityJobDefinitions",
            "sagemaker:ListModels",
            "sagemaker:ListMonitoringAlerts",
            "sagemaker:ListMonitoringSchedules",
            "sagemaker:ListNotebookInstanceLifecycleConfigs",
            "sagemaker:ListNotebookInstances",
            "sagemaker:ListOptimizationJobs",
            "sagemaker:ListPartnerApps",
            "sagemaker:ListPipelines",
            "sagemaker:ListProcessingJobs",
```

```
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListTagsForResource",
```

```
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serviceCatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:DescribeTagOption",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ListTagOptions",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
        "ses:ListArchives",
        "ses:ListConfigurationSets",
```

```
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListIngressPoints",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListRelays",
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
```

```
        "ssm-contacts:GetRotation",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListRotations",
        "ssm-contacts:ListTagsForResource",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListActivities",
```

```
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "textract:GetAdapter",
        "textract:ListAdapters",
        "textract:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWebApp",
        "transfer:DescribeWebAppCustomization",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
```

```
        "transfer:ListUsers",
        "transfer:ListWebApps",
        "transfer:ListWorkflows",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
```

```
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wisdom:GetAIGuardrail",
        "wisdom:ListAIGuardrails",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetSamplingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigSLRLogStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "AWSConfigSLRLogEventStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    },
    {
      "Sid" : "AWSConfigSLRApiGatewayStatementID",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes/*",
        "arn:aws:apigateway:*::/v2/apis",
        "arn:aws:apigateway:*::/v2/apis/*",
        "arn:aws:apigateway:*::/v2/apis/*/integrations",
        "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSConfigThirdPartyServiceRolePolicy

Descrizione: fornisce le autorizzazioni a AWS Config per inventariare e valutare la conformità delle risorse cloud di terze parti.

`AWSConfigThirdPartyServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 22 giugno 2026, 17:57 UTC
- Ora modificata: 22 giugno 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigThirdPartyServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AllowGetWebIdentityTokenByConfig",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "sts:IdentityTokenAudience" : [
            "api://AzureADTokenExchange"
          ]
        }
      }
    },
    {
      "Sid" : "AllowConfigActionsForRules",
      "Effect" : "Allow",
      "Action" : [
        "config:PutEvaluations",
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudwatchActionsForMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Config"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSConfigUserAccess

Descrizione: fornisce l'accesso all'utilizzo di AWS Config, inclusa la ricerca per tag sulle risorse e la lettura di tutti i tag. Ciò non fornisce l'autorizzazione per configurare AWS Config, che richiede privilegi amministrativi.

`AWSConfigUserAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSConfigUserAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 febbraio 2015, 19:38 UTC
- Ora modificata: 18 marzo 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
```

```
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

Connettore AWS

Descrizione: consente un ampio read/write accesso a TUTTI gli oggetti EC2, read/write l'accesso ai bucket S3 che iniziano con 'import-to-ec2-' e la possibilità di elencare tutti i bucket S3, affinché Connector importi le AWS VM per tuo conto.

`AWSConnector`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AWSConnector` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 febbraio 2015, 17:14 UTC
- Ora modificata: 28 settembre 2015, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Versione della politica

Versione della politica: v3 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::import-to-ec2-*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelConversionTask",
        "ec2:CancelExportTask",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:DetachVolume",
        "ec2:ImportInstance",
        "ec2:ImportVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CancelImportTask",
        "ec2:ImportSnapshot",
        "ec2:DescribeImportSnapshotTasks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSControlTowerAccountServiceRolePolicy

Descrizione: consente a AWS Control Tower di chiamare AWS servizi che forniscono la configurazione automatica degli account e la governance centralizzata per conto dell'utente.

`AWSControlTowerAccountServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 5 giugno 2023, 22:04 UTC
- Ora modificata: 20 maggio 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "events:source" : "aws.securityhub"
        },
        "ForAllValues:StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AllowDescribeOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*"
    },
    {
      "Sid" : "AllowControlTowerToPublishSecurityNotifications",
      "Effect" : "Allow",
      "Action" : "sns:publish",
      "Resource" : "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "AllowActionsForSecurityHubIntegration",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "Sid" : "AllowDeleteConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
    {
      "Sid" : "AllowPutConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
```

```
    {
      "Sid" : "AllowConfigTagResource",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Sid" : "AllowConfigRulesDescribe",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowControlTowerToCreateConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToManageConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:DescribeAggregateComplianceByConfigRules",
        "config:SelectAggregateResourceConfig"
```

```
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/config-aggregator-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToTagConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToPassAggregatorRoleToConfig",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "config.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "AllowDescribeConfigurationAggregators",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationAggregators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListDelegatedAdministratorsForConfig",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowListDescribeOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
```

```
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    },
    {
      "Sid" : "AllowBatchDescribeTypeConfigurationsForHookConfigFetch",
      "Effect" : "Allow",
      "Action" : "cloudformation:BatchDescribeTypeConfigurations",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSControlTowerCloudTrailRolePolicy

Descrizione: AWS Control Tower abilita AWS CloudTrail come best practice e fornisce questo ruolo a AWS CloudTrail. AWS CloudTrail assume questo ruolo per creare e pubblicare i log CloudTrail

`AWSControlTowerCloudTrailRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSControlTowerCloudTrailRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 novembre 2025, 21:19 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerCloudTrailRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogStream",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSControlTowerIdentityCenterManagementPolicy

Descrizione: Fornisce le autorizzazioni per gestire le risorse IAM Identity Center (iDC) negli account dei membri registrati a Control Tower AWS . La policy è associata al AWSControl TowerAdmin ruolo solo se il cliente ha optato per l'integrazione di IAM iDC nella AWS Control Tower Landing Zone.

`AWSControlTowerIdentityCenterManagementPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSControlTowerIdentityCenterManagementPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 3 ottobre 2025, 18:34 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerIdentityCenterManagementPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowIdentityCenterInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListPermissionSets"
      ],
      "Resource" : "arn:aws:sso:::instance/*"
    },
    {
      "Sid" : "AllowIdentityCenterManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations",
```

```
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:GetProfile",
        "sso:CreateProfile",
        "sso:UpdateProfile",
        "sso:GetTrust",
        "sso:CreateTrust",
        "sso:UpdateTrust",
        "sso:CreateApplicationInstance",
        "sso:GetApplicationInstance",
        "sso:GetSSOStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowIdentityCenterDirectoryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:SearchGroups",
        "sso-directory:CreateGroup",
        "sso-directory:SearchUsers",
        "sso-directory:CreateUser",
        "sso-directory:DescribeDirectory"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSControlTowerServiceRolePolicy

Descrizione: Fornisce l'accesso alle AWS risorse gestite o utilizzate da AWS Control Tower

`AWSControlTowerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSControlTowerServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 03 maggio 2019, 18:19 UTC
- Ora modificata: 20 maggio 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Versione della politica

Versione della politica: v21 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
```

```
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateTrail",
        "cloudtrail:DeleteTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail",
        "cloudtrail:PutEventSelectors",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*",
        "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-controltower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSControlTowerExecution",
        "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "ec2:DescribeAvailabilityZones",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "organizations:CreateAccount",
        "organizations:DescribeAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
```

```
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListRoots",
        "organizations:MoveAccount",
        "servicecatalog:AssociatePrincipalWithPortfolio"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
        "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
        "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator",
        "config:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws-control-tower" : "managed-by-control-tower"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com",
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:EnableRegion",
        "account:ListRegions",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
```

```
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    },
    {
      "Sid" : "AllowBatchDescribeTypeConfigurationsForHookConfigFetch",
      "Effect" : "Allow",
      "Action" : "cloudformation:BatchDescribeTypeConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationStackSetOrganizationsTrustedAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ActivateOrganizationsAccess",
        "cloudformation:DescribeOrganizationsAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSCostAndUsageReportAutomationPolicy

Descrizione: concede le autorizzazioni per descrivere l'organizzazione dell'account, creare bucket S3 per il programma MAP e applicarvi tag, creare un rapporto sui costi e sull'utilizzo e descrivere le definizioni del rapporto sui costi e sull'utilizzo.

`AWSCostAndUsageReportAutomationPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSCostAndUsageReportAutomationPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 01 novembre 2021, 21:27 UTC
- Ora modificata: 01 novembre 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:PutBucketTagging",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
```

```
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : "arn:aws:s3:::aws-map-cur-bucket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cur:PutReportDefinition",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions"
      ],
      "Resource" : "arn:aws:cur:*:*:definition/map-migrated-report"
    },
    {
      "Effect" : "Allow",
      "Action" : "cur:DescribeReportDefinitions",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataExchangeDataGrantOwnerFullAccess

Descrizione: consente ai proprietari di Data Grant di accedere alle azioni AWS Data Exchange utilizzando l'SDK Console di gestione AWS and.

`AWSDataExchangeDataGrantOwnerFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDataExchangeDataGrantOwnerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 ottobre 2024, 14:43 UTC
- Ora modificata: 24 ottobre 2024, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantOwnerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:UpdateDataSet",
        "dataexchange:GetDataSet",
        "dataexchange:DeleteDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:CreateRevision",
        "dataexchange:UpdateRevision",
        "dataexchange:GetRevision",
        "dataexchange:DeleteRevision",
        "dataexchange:RevokeRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:CreateAsset",
        "dataexchange:UpdateAsset",
        "dataexchange:GetAsset",
        "dataexchange:DeleteAsset",
        "dataexchange:ListRevisionAssets",
```

```
        "dataexchange:SendApiAsset",
        "dataexchange:CreateDataGrant",
        "dataexchange:GetDataGrant",
        "dataexchange:DeleteDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:PublishToDataGrant",
        "dataexchange:SendDataSetNotification",
        "dataexchange:TagResource",
        "dataexchange:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES",
            "IMPORT_ASSETS_FROM_LAKE_FORMATION_TAG_POLICY"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataExchangeDataGrantReceiverFullAccess

Descrizione: consente al destinatario di Data Grant di accedere alle azioni di AWS Data Exchange utilizzando l'SDK Console di gestione AWS and.

`AWSDataExchangeDataGrantReceiverFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDataExchangeDataGrantReceiverFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 ottobre 2024, 14:45 UTC
- Ora modificata: 24 ottobre 2024, 14:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantReceiverFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "dataexchange:GetDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:GetRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:GetAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:GetEventAction",
        "dataexchange:ListEventActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeDataGrantActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:AcceptDataGrant",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:GetReceivedDataGrant"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataExchangeFullAccess

Descrizione: concede l'accesso completo a AWS Data Exchange e alle AWS Marketplace azioni utilizzando l'SDK Console di gestione AWS and. Fornisce inoltre un accesso selezionato ai servizi correlati necessari per sfruttare appieno il AWS Data Exchange.

`AWSDataExchangeFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDataExchangeFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2019, 19:27 UTC
- Ora modificata: 24 giugno 2024, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceProviderActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
```

```
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataExchangeProviderFullAccess

Descrizione: concede al provider di dati l'accesso a AWS Data Exchange e alle AWS Marketplace azioni utilizzando l'SDK Console di gestione AWS and. Fornisce inoltre un accesso selezionato ai servizi correlati necessari per sfruttare appieno il AWS Data Exchange.

`AWSDataExchangeProviderFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDataExchangeProviderFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2019, 19:27 UTC
- Ora modificata: 15 agosto 2024, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:CreateRevision",
        "dataexchange:CreateAsset",
        "dataexchange:Get*",
        "dataexchange:Update*",
        "dataexchange:List*",
        "dataexchange:Delete*",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "dataexchange:PublishDataSet",
        "dataexchange:SendApiAsset",
        "dataexchange:RevokeRevision",
```

```
        "dataexchange:SendDataSetNotification",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
```

```
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
```

```
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataExchangeReadOnly

Descrizione: concede l'accesso in sola lettura a AWS Data Exchange e alle AWS Marketplace azioni utilizzando l' Console di gestione AWS SDK and.

`AWSDataExchangeReadOnly`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSDataExchangeReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2019, 19:27 UTC
- Ora modificata: 24 ottobre 2024, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetAsset",
        "dataexchange:GetDataSet",
        "dataexchange:GetEventAction",
        "dataexchange:GetJob",
        "dataexchange:GetRevision",
        "dataexchange:GetDataGrant",
        "dataexchange:GetReceivedDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListDataSets",
        "dataexchange:ListEventActions",
        "dataexchange:ListJobs",
        "dataexchange:ListRevisionAssets",
        "dataexchange:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:GetAgreementApprovalRequest",
```

```
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataExchangeServiceRolePolicyForLicenseManagement

Descrizione: consente l'accesso a AWS Data Exchange Servizi AWS e alle risorse utilizzate o gestite da AWS Data Exchange per la gestione delle licenze.

`AWSDataExchangeServiceRolePolicyForLicenseManagement`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 ottobre 2024, 14:54 UTC

- Ora modificata: 10 ottobre 2024, 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForLicenseManagement`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery

Descrizione: consente a AWS Data Exchange di leggere i dati relativi all' AWS organizzazione per determinare l'idoneità alla distribuzione delle licenze AWS Data Exchange Data Exchange.

`AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 ottobre 2024, 14:33 UTC
- Ora modificata: 10 ottobre 2024, 14:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAWSOrganizationsActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataExchangeSubscriberFullAccess

Descrizione: concede agli abbonati ai dati l'accesso a AWS Data Exchange e alle AWS Marketplace azioni utilizzando l'SDK Console di gestione AWS and. Fornisce inoltre un accesso selezionato ai servizi correlati necessari per sfruttare appieno il AWS Data Exchange.

`AWSDataExchangeSubscriberFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDataExchangeSubscriberFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2019, 19:27 UTC
- Ora modificata: 21 maggio 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
```

```
        "dataexchange:DeleteEventAction",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataLifecycleManagerServiceRole

Descrizione: fornisce le autorizzazioni appropriate a AWS Data Lifecycle Manager per intraprendere azioni sulle risorse AWS

`AWSDataLifecycleManagerServiceRole`è una policy gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSDataLifecycleManagerServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 luglio 2018, 19:34 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataLifecycleManagerServiceRoleForAMIManagement

Descrizione: Fornisce le autorizzazioni appropriate a AWS Data Lifecycle Manager per intraprendere azioni sulle risorse AWS per la gestione delle AMI

`AWSDataLifecycleManagerServiceRoleForAMIManagement`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSDataLifecycleManagerServiceRoleForAMIManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 21 ottobre 2020, 19:39 UTC

- Ora modificata: 19 agosto 2021, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImageDeprecation",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataLifecycleManagerSSMFullAccess

Descrizione: fornisce ad Amazon Data Lifecycle Manager l'autorizzazione a eseguire le azioni di Systems Manager necessarie per eseguire script pre e post su tutte le istanze Amazon EC2.

`AWSDataLifecycleManagerSSMFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSDataLifecycleManagerSSMFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 31 ottobre 2023, 20:29 UTC
- Ora modificata: 16 novembre 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggedSSMDocumentsOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DLMScriptsAccess" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSpecificAWSOwnedSSMDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
      ]
    },
    {
      "Sid" : "AllowAllEC2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataPipeline_FullAccess

Descrizione: fornisce accesso completo a Data Pipeline, accesso alle liste per i ruoli S3, DynamoDB, Redshift, RDS, SNS e IAM e accesso PassRole per i ruoli predefiniti.

`AWSDataPipeline_FullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSDataPipeline_FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 gennaio 2017, 23:14 UTC
- Ora modificata: 17 agosto 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
```

```
        "sns:Subscribe",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataPipeline_PowerUser

Descrizione: fornisce accesso completo a Data Pipeline, accesso alle liste per i ruoli S3, DynamoDB, Redshift, RDS, SNS e IAM e accesso PassRole per i ruoli predefiniti.

`AWSDataPipeline_PowerUser`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSDataPipeline_PowerUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 gennaio 2017, 23:16 UTC
- Ora modificata: 17 agosto 2017, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataSyncDiscoveryServiceRolePolicy

Descrizione: consente a DataSync Discovery di integrarsi con altri AWS servizi per conto dell'utente.

`AWSDataSyncDiscoveryServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 marzo 2023, 22:19 UTC
- Ora modificata: 20 marzo 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
```

```
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync:log-stream:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataSyncFullAccess

Descrizione: fornisce accesso completo AWS DataSync e accesso minimo alle sue dipendenze

`AWSDataSyncFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDataSyncFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 gennaio 2019, 19:40 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Versione della politica

Versione della politica: v16 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datasync:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "outposts:ListOutposts",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListRegionalBuckets",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "DataSyncPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datasync.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DataSyncCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/datasync.amazonaws.com/
AWSServiceRoleForDataSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "datasync.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataSyncSecretsManagerCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataSyncSecretsManagerAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataSyncReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a AWS DataSync

`AWSDataSyncReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDataSyncReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 gennaio 2019, 19:18 UTC

- Ora modificata: 30 giugno 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:Describe*",
        "datasync:List*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDataSyncServiceRolePolicy

Descrizione: consente DataSync l'integrazione con altri AWS servizi per tuo conto

`AWSDataSyncServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 9 ottobre 2024, 17:45 UTC
- Ora modificata: 15 aprile 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncCloudWatchLogCreateAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Sid" : "DataSyncCloudWatchLogStreamUpdateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*:log-stream:*"
      ]
    },
    {
      "Sid" : "DataSyncSecretsManagerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeadlineCloud-FleetWorker

Descrizione: fornisce ai lavoratori di AWS Deadline Cloud l'accesso all'esecuzione delle attività in una fattoria.

`AWSDeadlineCloud-FleetWorker`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeadlineCloud-FleetWorker` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 17:21 UTC
- Ora modificata: 01 aprile 2024, 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunTasksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForWorker",
        "deadline:UpdateWorker",
```

```
        "deadline:UpdateWorkerSchedule",
        "deadline:BatchGetJobEntity",
        "deadline:AssumeQueueRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeadlineCloud-UserAccessFarms

Descrizione: fornisce l'accesso alla workstation utente alle farm AWS Deadline Cloud con Read-Only autorizzazioni limitate per chiamare altri servizi necessari. Allega questa policy al ruolo utente associato al tuo studio.

`AWSDeadlineCloud-UserAccessFarms`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeadlineCloud-UserAccessFarms` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 16:54 UTC
- Ora modificata: 29 maggio 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "deadline:GetMonitorSettings",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:CreateBudget",
        "deadline:DeleteBudget",
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue",
```

```
        "deadline:GetBudget",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:ListBudgets",
        "deadline:StartSessionsStatisticsAggregation",
        "deadline:UpdateBudget"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
```

```
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarmMembers",
        "deadline:ListFleetMembers",
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
```

```
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
```

```
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetVolume",
        "deadline:GetWorker",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:ListVolumes",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeadlineCloud-UserAccessFleets

Descrizione: fornisce l'accesso alla workstation utente alle flotte di AWS Deadline Cloud con Read-Only autorizzazioni limitate per chiamare altri servizi necessari. Allega questa policy al ruolo utente associato al tuo studio.

`AWSDeadlineCloud-UserAccessFleets`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeadlineCloud-UserAccessFleets` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 17:01 UTC
- Ora modificata: 29 maggio 2026, 21:27 UTC

- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet",
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "deadline:FleetMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFleetMembers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:GetFleet",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetVolume",
        "deadline:GetWorker",
```

```
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionsForWorker",
        "deadline:ListVolumes",
        "deadline:ListWorkers",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFleets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeadlineCloud-UserAccessJobs

Descrizione: fornisce all'utente l'accesso alla workstation ai job di AWS Deadline Cloud con autorizzazioni di sola lettura limitate per chiamare altri servizi necessari. Allega questa policy al ruolo utente associato al tuo studio.

`AWSDeadlineCloud-UserAccessJobs`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeadlineCloud-UserAccessJobs` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 17:05 UTC
- Ora modificata: 07 ottobre 2024, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
```

```
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListTasks",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeadlineCloud-UserAccessQueues

Descrizione: fornisce all'utente l'accesso alla workstation alle code di AWS Deadline Cloud con autorizzazioni di sola lettura limitate per chiamare altri servizi necessari. Allega questa policy al ruolo utente associato al tuo studio.

`AWSDeadlineCloud-UserAccessQueues`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeadlineCloud-UserAccessQueues` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 17:10 UTC
- Ora modificata: 07 ottobre 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
```

```
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
```

```
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeadlineCloud-WorkerHost

Descrizione: consente agli host di lavoratori di AWS Deadline Cloud di entrare a far parte di una flotta in una fattoria.

`AWSDeadlineCloud-WorkerHost`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeadlineCloud-WorkerHost` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2024, 17:28 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "TagWorkerPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:TagResource"
      ],
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*/worker/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    },
    {
      "Sid" : "ListFleetTagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListTagsForResource"
      ],
```

```
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeepLensLambdaFunctionAccessPolicy

Descrizione: questa politica specifica le autorizzazioni richieste dalle funzioni lambda DeepLens amministrative eseguite su un dispositivo DeepLens

`AWSDeepLensLambdaFunctionAccessPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSDeepLensLambdaFunctionAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 15:47 UTC
- Ora modificata: 11 giugno 2019, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*/*",
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeepLensServiceRolePolicy

Descrizione: concede AWS DeepLens l'accesso alle risorse e ai ruoli necessari e alle relative dipendenze Servizi AWS, tra cui IoT, S3 e GreenGrass Lambda DeepLens . AWS

`AWSDeepLensServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSDeepLensServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 29 novembre 2017, 15:46 UTC
- Ora modificata: 25 settembre 2019, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
```

```
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIoTAttachCertificatePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "DeepLensIoTDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTEndpointAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensCreateS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIAMPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeepLensIAMLambdaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepLens*",
        "arn:aws:iam::*:role/service-role/AWSDeepLens*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DeepLensGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
```

```
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
```

```
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaAdminFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:deeplens*"
      ]
    },
    {
```

```
      "Sid" : "DeepLensLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:DeleteStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/deeplens*/*"
```

```
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeepRacerAccountAdminAccess

Descrizione: accesso DeepRacer amministrativo a tutte le azioni, inclusa la commutazione tra la modalità multiutente e quella a utente singolo.

`AWSDeepRacerAccountAdminAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSDeepRacerAccountAdminAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 ottobre 2021, 01:27 UTC
- Ora modificata: 28 ottobre 2021, 01:27 UTC

- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeepRacerCloudFormationAccessPolicy

Descrizione: consente di CloudFormation creare e gestire AWS pile e risorse per tuo conto.

`AWSDeepRacerCloudFormationAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeepRacerCloudFormationAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 febbraio 2019, 21:59 UTC
- Ora modificata: 14 giugno 2019, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
```

```
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AWSDeepRacerLambdaAccessRole",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:TagResource",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:DeleteBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
```

```
        "arn:aws:s3:::*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:CreateSimulationApplication",
        "robomaker:CreateSimulationApplicationVersion",
        "robomaker:DeleteSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListSimulationApplications",
        "robomaker:TagResource",
        "robomaker:UpdateSimulationApplication"
      ],
      "Resource" : [
        "arn:aws:robomaker:*:*:/createSimulationApplication",
        "arn:aws:robomaker:*:*:simulation-application/deepracer*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeepRacerDefaultMultiUserAccess

Descrizione: accesso utente DeepRacer MultiUser predefinito per utilizzare deepracer in modalità multiutente

`AWSDeepRacerDefaultMultiUserAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSDeepRacerDefaultMultiUserAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 ottobre 2021, 01:27 UTC
- Ora modificata: 28 ottobre 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:Add*",
        "deepracer:Remove*",
        "deepracer:Create*",
        "deepracer:Perform*",
        "deepracer:Clone*",
        "deepracer:Get*",
        "deepracer:List*",
        "deepracer:Edit*",
        "deepracer:Start*",
        "deepracer:Set*",
        "deepracer:Update*",
        "deepracer:Delete*",
        "deepracer:Stop*",
        "deepracer:Import*",
        "deepracer:Tag*",
        "deepracer:Untag*"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "false"
        },
        "Bool" : {
          "deepracer:MultiUser" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:GetAccountConfig",
        "deepracer:GetTrack",
        "deepracer:ListTracks",
        "deepracer:TestRewardFunction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "deepracer:Admin*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeepRacerFullAccess

Descrizione: Fornisce accesso completo a AWS DeepRacer. Fornisce inoltre un accesso selezionato ai servizi correlati (ad esempio, S3).

`AWSDeepRacerFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeepRacerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 ottobre 2020, 22:03 UTC
- Ora modificata: 5 ottobre 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*",
        "arn:aws:s3:::*DeepRacer*/*",
        "arn:aws:s3:::*Deepracer*/*",
        "arn:aws:s3:::*deepracer*/*",
        "arn:aws:s3:::dr-*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeepRacerRoboMakerAccessPolicy

Descrizione: consente di RoboMaker creare le risorse necessarie e chiamare AWS i servizi per conto dell'utente.

`AWSDeepRacerRoboMakerAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeepRacerRoboMakerAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 febbraio 2019, 21:59 UTC
- Ora modificata: 28 febbraio 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs",
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeepRacerServiceRolePolicy

Descrizione: consente di DeepRacer creare le risorse necessarie e chiamare AWS i servizi per conto dell'utente.

`AWSDeepRacerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeepRacerServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 28 febbraio 2019, 21:58 UTC

- Ora modificata: 12 giugno 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*",
        "sagemaker:*",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
```

```
        "cloudformation:DetectStackDrift",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:DescribeStackResourceDrifts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      },
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepRacer*",
        "arn:aws:iam::*:role/service-role/AWSDeepRacer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
```

```
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*",
        "arn:aws:lambda:*:*:function:*dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
```

```
        "kinesisvideo:DeleteStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetHLSStreamingSessionURL",
        "kinesisvideo:GetMedia",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDenyAll

Descrizione: nega tutti gli accessi.

`AWSDenyAll`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDenyAll` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 maggio 2019, 22:36 UTC
- Ora modificata: 18 dicembre 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAll",
      "Effect" : "Deny",
      "Action" : [
        "*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeviceFarmFullAccess

Descrizione: Fornisce l'accesso completo a tutte le operazioni di AWS Device Farm.

`AWSDeviceFarmFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDeviceFarmFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 luglio 2015, 16:37 UTC
- Ora modificata: 13 luglio 2015, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "devicefarm:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeviceFarmServiceRolePolicy

Descrizione: Concedi le autorizzazioni a AWS Device Farm per chiamare EC2 Network per tuo APIs conto.

`AWSDeviceFarmServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 settembre 2022, 21:02 UTC
- Ora modificata: 20 settembre 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDeviceFarmTestGridServiceRolePolicy

Descrizione: concedi le autorizzazioni a AWS Device Farm per chiamare EC2 per tuo APIs conto.

`AWSDeviceFarmTestGridServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 maggio 2021, 22:01 UTC
- Ora modificata: 26 maggio 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDirectConnectFullAccess

Descrizione: Fornisce l'accesso completo a AWS Direct Connect tramite Console di gestione AWS.

`AWSDirectConnectFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDirectConnectFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 30 aprile 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDirectConnectReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura a AWS Direct Connect tramite Console di gestione AWS.

`AWSDirectConnectReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDirectConnectReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 18 maggio 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDirectConnectServiceRolePolicy

Descrizione: Fornisce l'autorizzazione AWS Direct Connect per creare e gestire AWS risorse per tuo conto.

`AWSDirectConnectServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 gennaio 2021, 18:35 UTC
- Ora modificata: 14 gennaio 2021, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDirectoryServiceDataFullAccess

Descrizione: fornisce l'accesso completo ai dati del AWS Directory Service.

`AWSDirectoryServiceDataFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDirectoryServiceDataFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 settembre 2024, 21:45 UTC
- Ora modificata: 18 settembre 2024, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:AddGroupMember",
        "ds-data:CreateGroup",
        "ds-data:CreateUser",
        "ds-data:DeleteGroup",
        "ds-data:DeleteUser",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:DisableUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
```

```
        "ds-data:ListUsers",
        "ds-data:RemoveGroupMember",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers",
        "ds-data:UpdateGroup",
        "ds-data:UpdateUser"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDirectoryServiceDataReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura ai dati del AWS Directory Service

`AWSDirectoryServiceDataReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDirectoryServiceDataReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 settembre 2024, 22:00 UTC
- Ora modificata: 18 settembre 2024, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDirectoryServiceFullAccess

Descrizione: fornisce l'accesso completo a AWS Directory Service.

`AWSDirectoryServiceFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDirectoryServiceFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 02 aprile 2024, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectoryServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeSecurityGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "iam:ListRoles",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DirectoryServiceEventTopic",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
    },
    {
      "Sid" : "DirectoryServiceOrganizations",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "organizations:ServicePrincipal" : "ds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DirectoryServiceTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDirectoryServiceReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura al AWS Directory Service.

`AWSDirectoryServiceReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDirectoryServiceReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 25 settembre 2018, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDirectoryServiceServiceRolePolicy

Descrizione: Criteri per il ruolo collegato al servizio Directory Service

`AWSDirectoryServiceServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 11 luglio 2025, 00:22 UTC
- Ora modificata: 11 luglio 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectoryServiceServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDiscoveryContinuousExportFirehosePolicy

Descrizione: fornisce accesso in scrittura alle AWS risorse necessarie per AWS Discovery Continuous Export

`AWSDiscoveryContinuousExportFirehosePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSDiscoveryContinuousExportFirehosePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 agosto 2018, 18:29 UTC
- Ora modificata: 08 giugno 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-application-discovery-service-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/firehose:log-
stream:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDMSFleetAdvisorServiceRolePolicy

Descrizione: consente a DMS Fleet Advisor di gestire le CloudWatch metriche per tuo conto.

`AWSDMSFleetAdvisorServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 6 marzo 2023, 09:10 UTC
- Ora modificata: 6 marzo 2023, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
```

```
      }
    }
  }
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSDMSServerlessServiceRolePolicy

Descrizione: concede le autorizzazioni AWS DMS Serverless per creare e gestire le risorse DMS del tuo account per tuo conto

`AWSDMSServerlessServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 maggio 2023, 20:28 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:ModifyReplicationTask",
        "dms:DeleteReplicationTask",
        "dms:ModifyReplicationInstance",
        "dms:DeleteReplicationInstance"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
```

```
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id3",
      "Effect" : "Allow",
      "Action" : [
        "dms:TestConnection",
        "dms:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:endpoint:*"
      ]
    },
    {
      "Sid" : "id4",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObjectTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketLocation",
```

```
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id6",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTaskAssessmentRun"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEC2CapacityManagerServiceRolePolicy

Descrizione: consente a EC2 Capacity Manager di gestire le risorse di capacità e di integrarsi con AWS Organizations per tuo conto.

`AWSEC2CapacityManagerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 9 ottobre 2025, 22:04 UTC
- Ora modificata: 09 ottobre 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityManagerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsDefaultReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsListDelegatedAdministratorsAction",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "ec2.capacitymanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEC2CapacityReservationFleetRolePolicy

Descrizione: consente al servizio EC2 CapacityReservation Fleet di gestire le prenotazioni di capacità

`AWSEC2CapacityReservationFleetRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 29 settembre 2021, 14:43 UTC
- Ora modificata: 3 marzo 2025, 23:22 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateCapacityReservation",
        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:CapacityReservationFleet" : "arn:aws:ec2:*:*:capacity-reservation-fleet/
crf-*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateCapacityReservation"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEC2FleetServiceRolePolicy

Descrizione: consente a EC2 Fleet di avviare e gestire le istanze.

`AWSEC2FleetServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 marzo 2018, 00:08 UTC
- Ora modificata: 04 maggio 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEC2SpotFleetServiceRolePolicy

Descrizione: consente a EC2 Spot Fleet di avviare e gestire le istanze del parco istanze spot

`AWSEC2SpotFleetServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 23 ottobre 2017, 19:13 UTC
- Ora modificata: 16 marzo 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*",
        "arn:aws:ec2:*:*:spot-fleet-request/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEC2SpotServiceRolePolicy

Descrizione: consente a EC2 Spot di avviare e gestire istanze spot

`AWSEC2SpotServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 settembre 2017, 18:51 UTC
- Ora modificata: 12 dicembre 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "ec2:InstanceMarketType" : "spot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEC2SqlHaInstancePolicy

Descrizione: autorizzazioni dell'istanza Amazon EC2 per consentire al servizio EC2 SQL High Availability di rilevare lo stato di alta disponibilità dell'istanza tramite il profilo dell'istanza EC2.

`AWSEC2SqlHaInstancePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSEC2SqlHaInstancePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2025, 01:49 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2SqlHaInstancePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSEc2SqlHa" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEC2SqlHaServiceRolePolicy

Descrizione: autorizzazioni del servizio EC2 SQL High Availability per rilevare le istanze standby/passive

`AWSEC2SqlHaServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 13 novembre 2025, 01:34 UTC
- Ora modificata: 13 novembre 2025, 01:34 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SqlHaServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMSendCommandToTaggedInstances",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendCommandOfOwnedDoc",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-DetectSqlHa*"
      ]
    },
    {
      "Sid" : "AllowSSMNonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
```

```
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2NonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventsMutateManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2sqlha.amazonaws.com",
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    },
    {
      "Sid" : "AllowEventsNonMutatingManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEC2VssRestorePolicy

Descrizione: concede ad Amazon EC2 AWS e SSM le autorizzazioni per ripristinare il database SQL Server da istantanee coerenti dell'applicazione create da VSS. AWS

`AWSEC2VssRestorePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSEC2VssRestorePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 marzo 2026, 23:12 UTC
- Ora modificata: 25 marzo 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssRestorePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "CreateVolumeAccessVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        },
        "ArnLike" : {
          "ec2:ParentSnapshot" : "arn:aws:ec2:*:*:snapshot/*"
        }
      }
    },
    {
      "Sid" : "CreateVolumeAccessSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateVolumeWithTagging",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume"
        }
      }
    },
    {
      "Sid" : "AttachVolumeAccessVolume",
      "Effect" : "Allow",
      "Action" : "ec2:AttachVolume",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "AttachVolumeAccessInstance",
      "Effect" : "Allow",
      "Action" : "ec2:AttachVolume",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumes",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSnapshots",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSnapshots",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceAttribute",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "SsmAutomationRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmRunCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AWSEC2-PrepareVssRestore",
        "arn:aws:ssm:*:*:document/AWSEC2-RunVssRestoreForSqlDatabase"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEC2VssSnapshotPolicy

Descrizione: questa policy è associata al ruolo IAM associato alle istanze Windows di Amazon EC2 per consentire alla soluzione Amazon EC2 VSS di creare e aggiungere tag ad Amazon Machine Images (AMI) e agli snapshot EBS.

`AWSEC2VssSnapshotPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSEC2VssSnapshotPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 marzo 2024, 16:32 UTC
- Ora modificata: 20 novembre 2024, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceInfo",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
```

```
    {
      "Sid" : "CreateSnapshotsAccessInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "CreateImageWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateImageAccessInstance",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateImage",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsAfterResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppConsistent",
```

```
            "Device"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeImagesAndSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSECRPullThroughCache_ServiceRolePolicy

Descrizione: consente l'accesso ai AWS servizi e alle risorse utilizzati o gestiti da AWS ECR pull through cache

`AWSECRPullThroughCache_ServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo

- Ora di creazione: 26 novembre 2021, 21:51 UTC
- Ora modificata: 12 maggio 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage",
        "ecr:BatchGetImage",
        "ecr:BatchImportUpstreamImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetImageCopyStatus"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkCustomPlatformforEC2Role

Descrizione: autorizza l'istanza nel tuo ambiente di creazione di piattaforme personalizzate ad avviare un'istanza EC2, creare snapshot e AMI EBS, trasmettere i log ad Amazon Logs e archiviare artefatti in CloudWatch Amazon S3.

`AWSElasticBeanstalkCustomPlatformforEC2Role`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkCustomPlatformforEC2Role` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 febbraio 2017, 22:50 UTC
- Ora modificata: 21 febbraio 2017, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Access",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateKeypair",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteKeypair",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:GetPasswordData",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
```

```
        "ec2:ModifySnapshotAttribute",
        "ec2:RegisterImage",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/platform/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkEKSImageBuild

Descrizione: autorizzazioni necessarie a Elastic Beanstalk per creare immagini di container per conto del cliente.

`AWSElasticBeanstalkEKSImageBuild`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkEKSImageBuild` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 luglio 2026, 21:27 UTC
- Ora modificata: 02 luglio 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSImageBuild`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3SourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRPublicAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRRepositoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:PutImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
```

```
        "ecr:CompleteLayerUpload"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkEKSObservability

Descrizione: autorizzazioni di osservabilità per ambienti Elastic Beanstalk in esecuzione nel cluster Elastic Kubernetes Service

`AWSElasticBeanstalkEKSObservability`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkEKSObservability` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 luglio 2026, 21:27 UTC
- Ora modificata: 02 luglio 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSObservability`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FluentBitS3Plugin",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-logs-*",
        "arn:aws:s3:::elasticbeanstalk-logs-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "APSCreateWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "APSManageWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:DeleteWorkspace",
        "aps:Describe*"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "APSRemoteWrite",
      "Effect" : "Allow",
      "Action" : [
        "aps:RemoteWrite"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkEKSTagging

Descrizione: autorizzazioni necessarie per passare attraverso i tag alle risorse create dai controllori EKS

`AWSElasticBeanstalkEKSTagging`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkEKSTagging` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 luglio 2026, 21:27 UTC
- Ora modificata: 02 luglio 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSTagging`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Compute",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-node-class-name" : "*",
          "aws:RequestTag/eks:kubernetes-node-pool-name" : "*"
        }
      }
    },
    {
      "Sid" : "Storage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
```

```
    {
      "Sid" : "Networking",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-cni-node-name" : "*"
        }
      }
    },
    {
      "Sid" : "LoadBalancer",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateRule",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Sid" : "ShieldProtection",
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
```

```
        }
      }
    },
    {
      "Sid" : "ShieldTagResource",
      "Effect" : "Allow",
      "Action" : [
        "shield:TagResource"
      ],
      "Resource" : "arn:aws:shield::*:protection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkEnhancedHealth

Descrizione: politica di AWS Elastic Beanstalk Service per il sistema di monitoraggio della salute

`AWSElasticBeanstalkEnhancedHealth`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkEnhancedHealth` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 8 febbraio 2016, 23:17 UTC
- Ora modificata: 09 aprile 2018, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:GetConsoleOutput",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeSecurityGroups",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeNotificationConfigurations",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkMaintenance

Descrizione: AWS politica del ruolo del servizio Elastic Beanstalk che concede autorizzazioni limitate per aggiornare le risorse per tuo conto a fini di manutenzione.

`AWSElasticBeanstalkMaintenance`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 11 gennaio 2019, 23:22 UTC
- Ora modificata: 29 aprile 2024, 21:48 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

Descrizione: questa policy riguarda il ruolo del servizio AWS Elastic Beanstalk utilizzato per eseguire aggiornamenti gestiti degli ambienti Elastic Beanstalk. Questa politica non deve essere associata ad altri utenti o ruoli. La policy concede ampie autorizzazioni per creare e gestire risorse su una serie di AWS servizi AutoScaling, tra cui EC2, ECS, Elastic Load Balancing e. CloudFormation Questa policy consente inoltre il trasferimento di qualsiasi ruolo IAM utilizzabile con tali servizi.

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 marzo 2021, 22:18 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
```

```
        "autoscaling:DescribeScheduledActions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2BroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteSecurityGroup",
```

```
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2RunInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "EC2TerminateInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "ECSBroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ECSDeleteClusterOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ecs:DeleteCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Sid" : "ASGOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFNOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
```

```
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "ELBOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*"
      ]
    },
    {
      "Sid" : "CWLogsOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "S3ObjectOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
```

```
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3BucketOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "SNSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Sid" : "SQSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Sid" : "CWPutMetricAlarmOperationPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances",
            "AllocateAddress"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Descrizione: AWS politica del ruolo del servizio Elastic Beanstalk che concede autorizzazioni limitate agli aggiornamenti gestiti.

`AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 novembre 2019, 22:35 UTC
- Ora modificata: 13 marzo 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SingleInstanceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ElasticBeanstalkAPIs",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:List*",
        "ec2:Describe*",
        "autoscaling:Describe*",
        "elasticloadbalancing:Describe*",
        "logs:DescribeLogGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
```

```
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CancelUpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
```

```
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
    },
    {
      "Sid" : "EC2LaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*"
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances",
            "AllocateAddress"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkMulticontainerDocker

Descrizione: fornisci alle istanze del tuo ambiente Docker multicontainer l'accesso per utilizzare Amazon EC2 Container Service per gestire le attività di distribuzione dei container.

`AWSElasticBeanstalkMulticontainerDocker`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkMulticontainerDocker` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 febbraio 2016, 23:15 UTC
- Ora modificata: 29 aprile 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DiscoverPollEndpoint",
        "ecs:StartTelemetrySession",
        "ecs:RegisterContainerInstance",
        "ecs:DeregisterContainerInstance",
        "ecs:DescribeContainerInstances",
        "ecs:Submit*",
        "ecs:DescribeTasks"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterContainerInstance",
            "StartTask"
          ]
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*::foundation-model/amazon.nova-*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
        "arn:aws:bedrock:*:*:inference-profile/*amazon.nova-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
```

```
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrock",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkReadOnly

Descrizione: concede autorizzazioni di sola lettura. Consente esplicitamente agli operatori di ottenere l'accesso diretto per recuperare informazioni sulle risorse relative alle applicazioni Elastic AWS Beanstalk.

`AWSElasticBeanstalkReadOnly`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 gennaio 2021, 19:02 UTC
- Ora modificata: 19 maggio 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAPIs",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
```

```
        "cloudformation:ValidateTemplate",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeDBSnapshots",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "AllowCloudWatchLogsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "AllowCloudWatchLogsRead",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkRoleCore

Descrizione: AWSElastic BeanstalkRoleCore (ruolo operativo Elastic Beanstalk) Consente il funzionamento principale di un ambiente di servizi Web.

`AWSElasticBeanstalkRoleCore`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkRoleCore` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:48 UTC
- Ora modificata: 30 aprile 2024, 00:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/awseb-e-*"
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress",
        "ec2:AllocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:RevokeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:DeleteLaunchTemplate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LTRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:*LoadBalancer*",
```

```
        "autoscaling:*AutoScalingGroup",
        "autoscaling:*LaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
      ]
    },
    {
      "Sid" : "ASGPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EBSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*/*",
        "arn:aws:s3:::elasticbeanstalk-env-resources-*/*"
      ]
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CancelUpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
```

```
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Create*",
        "elasticloadbalancing:Delete*",
        "elasticloadbalancing:Modify*",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*"
      ]
    },
    {
      "Sid" : "ListAPIs",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "logs:Describe*",
        "ec2:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "elasticloadbalancing:Describe*",
        "rds:Describe*",
        "sns:List*",
        "iam:List*",
```

```
        "acm:Describe*",
        "acm:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkRoleCWL

Descrizione: (ruolo operativo Elastic Beanstalk) Consente a un ambiente di gestire CloudWatch i gruppi di log di Amazon Logs.

`AWSElasticBeanstalkRoleCWL`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkRoleCWL` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:49 UTC
- Ora modificata: 5 giugno 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkRoleECS

Descrizione: (ruolo operativo Elastic Beanstalk) Consente a un ambiente Docker multicontainer di gestire i cluster Amazon ECS.

`AWSElasticBeanstalkRoleECS`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkRoleECS` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:47 UTC
- Ora modificata: 23 marzo 2023, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkRoleRDS

Descrizione: (ruolo operativo Elastic Beanstalk) Consente a un ambiente di integrare un'istanza Amazon RDS.

`AWSElasticBeanstalkRoleRDS`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkRoleRDS` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:46 UTC
- Ora modificata: 5 giugno 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBSecurityGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:ModifyDBInstance",
```

```
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:db:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkRoleSNS

Descrizione: (ruolo operativo Elastic Beanstalk) Consente a un ambiente di abilitare l'integrazione degli argomenti di Amazon SNS.

`AWSElasticBeanstalkRoleSNS`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkRoleSNS` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:46 UTC
- Ora modificata: 5 giugno 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBeanstalkManageSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:DeleteTopic"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
      ]
    },
    {
      "Sid" : "AllowSNSPublish",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkRoleWorkerTier

Descrizione: (ruolo operativo Elastic Beanstalk) Consente a un livello di ambiente di lavoro di creare una tabella Amazon DynamoDB e una coda Amazon SQS.

`AWSElasticBeanstalkRoleWorkerTier`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkRoleWorkerTier` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2020, 21:43 UTC
- Ora modificata: 5 giugno 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
```

```
      ],
      "Resource" : "arn:aws:sqs:*:*:awseb-e-*"
    },
    {
      "Sid" : "AllowDDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awseb-e-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkService

Descrizione: questa politica si trova su un percorso obsoleto. Consulta la documentazione come guida: -servicerole.html. https://docs.aws.amazon.com/elasticbeanstalk/ latest/dg/iam AWS Politica del ruolo di Elastic Beanstalk Service che concede le autorizzazioni per creare e gestire risorse (AutoScalingad esempio: EC2, CloudFormation S3, ELB, ecc.) per tuo conto.

`AWSElasticBeanstalkService`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkService` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 11 aprile 2016, 20:27 UTC
- Ora modificata: 10 maggio 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Versione della politica

Versione della politica: v17 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowDeleteCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3OperationsOnElasticBeanstalkBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowELBAddTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudwatch:PutMetricAlarm",
        "ec2:AssociateAddress",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
```

```
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeVpcClassicLink",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:TerminateInstances",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "iam:ListRoles",
        "iam:PassRole",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
```

```
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:ListBucket",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:SetTopicAttributes",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkServiceRolePolicy

Descrizione: politica AWS Elastic Beanstalk Service Linked Role che concede le autorizzazioni per creare e gestire risorse (ad esempio: EC2 AutoScaling, S3, ELB, ecc.) per CloudFormation conto dell'utente.

`AWSElasticBeanstalkServiceRolePolicy`è una policy gestita. AWS

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 13 settembre 2017, 23:46 UTC
- Ora modificata: 3 agosto 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Versione della politica

Versione della politica: v7 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationReadOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
```

```
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:PutNotificationConfiguration",
        "ec2:DescribeInstanceStatus",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "lambda:GetFunction",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOperationsOnHealthStreamingLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DeleteLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "EBEKSGeneralOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
```

```
        "acm:ListTagsForCertificate",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:DescribeRepositories",
        "ecr:ListTagsForResource",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "iam:GetRole",
        "codebuild:ListProjects",
        "codebuild:BatchGetProjects",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:DescribeConfigurationSettings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSDefaultHTTPSCertCreate",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:environment-id" : "false"
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSDefaultHTTPSCertModifyDelete",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSSubnetTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "kubernetes.io/role/elb",
            "kubernetes.io/role/internal-elb"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSIamCreateServiceLinkedRole",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EBEKSIamPermissionsImageBuild",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "codebuild.amazonaws.com",
            "eks.amazonaws.com",
            "ec2.amazonaws.com",
            "pods.eks.amazonaws.com",
            "elasticbeanstalk.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EBEKSS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSEKSClusterManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCluster",
        "eks:DeleteCluster",
        "eks:DescribeCluster",
        "eks:DescribeUpdate",
        "eks:CreateAccessEntry",
        "eks:DeleteAccessEntry",
        "eks:CreateAddon",
        "eks:CreatePodIdentityAssociation",
        "eks:ListPodIdentityAssociations"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/beanstalk-cluster*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSEKSAddonManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:DescribeAddon",
        "eks:UpdateAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/beanstalk-cluster*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "EBEKSEKSAccessEntryManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/beanstalk-cluster*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSEKSPodIdentityManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeletePodIdentityAssociation",
        "eks:DescribePodIdentityAssociation",
        "eks:UpdatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/beanstalk-cluster*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSCodeBuildProjectManagement",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject",
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:BatchGetProjects"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "EBEKSECRRepositoryManagement",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DescribeRepositories",
        "ecr:DescribeImages",
        "ecr:PutLifecyclePolicy",
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSCFNStackManagementImageBuild",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/elasticbeanstalk-*-image-build",
        "arn:aws:cloudformation:*:*:stack/elasticbeanstalk-*-image-build/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSCFNStackManagementClusterSetup",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
```

```
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/beanstalk-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSAPSCreateWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSAPSManageWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:DeleteWorkspace",
        "aps:Describe*"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk"
        }
      }
    },
```

```
    {
      "Sid" : "EBEKSAPSRemoteWrite",
      "Effect" : "Allow",
      "Action" : [
        "aps:RemoteWrite"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk"
        }
      }
    },
    {
      "Sid" : "EBEKSCreateDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : "arn:aws:cloudwatch::*:dashboard/ElasticBeanstalk-Observability-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbLoadBalancerWrite",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateTargetGroup",
```

```
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbTargetGroupModifyDelete",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbListenerRuleCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:environment-id" : "false"
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbListenerRuleDelete",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteRule"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:byo-alb-arn" : "false",
          "aws:RequestTag/elasticbeanstalk:managed" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2CreateSecurityGroupVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:byo-alb-arn" : "false",
          "aws:RequestTag/elasticbeanstalk:managed" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2SecurityGroupEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:byo-alb-arn" : "false",
          "aws:ResourceTag/elasticbeanstalk:managed" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "ECRTagMutation",
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:application-name" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CodeBuildTagMutation",
      "Effect" : "Allow",
      "Action" : "codebuild:UpdateProject",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:application-name" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagMutation",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:RemoveTagsFromCertificate",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkWebTier

Descrizione: fornisci alle istanze del tuo ambiente di server Web l'accesso per caricare file di registro su Amazon S3.

`AWSElasticBeanstalkWebTier`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkWebTier` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 febbraio 2016, 23:08 UTC
- Ora modificata: 29 aprile 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*::foundation-model/amazon.nova-*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
        "arn:aws:bedrock:*:*:inference-profile/*amazon.nova-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
```

```
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrock",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticBeanstalkWorkerTier

Descrizione: consenti alle istanze del tuo ambiente di lavoro di accedere per caricare file di log su Amazon S3, usare Amazon SQS per monitorare la coda di lavoro della tua applicazione, usare Amazon DynamoDB per eleggere i leader e Amazon per pubblicare metriche per il monitoraggio dello stato. CloudWatch

`AWSElasticBeanstalkWorkerTier`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticBeanstalkWorkerTier` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 8 febbraio 2016, 23:12 UTC
- Ora modificata: 29 aprile 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MetricsAccess",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "QueueAccess",
      "Action" : [
        "sqs:ChangeMessageVisibility",
```

```
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "DynamoPeriodicTasks",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:UpdateItem"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*-stack-AWSEBWorkerCronLeaderRegistry*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*::foundation-model/amazon.nova-*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
        "arn:aws:bedrock:*:*:inference-profile/*amazon.nova-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
```

```
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrock",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryAgentInstallationPolicy

Descrizione: questa policy consente di installare il AWS Replication Agent, che viene utilizzato con AWS Elastic Disaster Recovery (DRS) per ripristinare i server esterni. AWS Allega questa policy agli utenti o ai ruoli IAM di cui fornisci le credenziali durante la fase di installazione dell'agente di replica. AWS

`AWSElasticDisasterRecoveryAgentInstallationPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryAgentInstallationPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2021, 10:37 UTC
- Ora modificata: 27 novembre 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateRecoveryInstanceForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSAgentInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy3",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateRecoveryInstanceForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy4",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy5",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryAgentPolicy

Descrizione: questa policy consente di utilizzare l'agente di AWS replica, utilizzato con AWS Elastic Disaster Recovery (DRS) per ripristinare i server di origine. AWS Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

`AWSElasticDisasterRecoveryAgentPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryAgentPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 novembre 2021, 10:32 UTC
- Ora modificata: 27 novembre 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentPolicy1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/${aws:SourceIdentity}"
    },
    {
      "Sid" : "DRSAgentPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryConsoleFullAccess

Descrizione: questa policy fornisce l'accesso completo a tutto il pubblico APIs di AWS Elastic Disaster Recovery (DRS), nonché le autorizzazioni per leggere le informazioni su KMS key, License Manager, Resource Groups, Elastic Load Balancing, IAM ed EC2. Allega questa policy ai tuoi utenti o ruoli IAM.

`AWSElasticDisasterRecoveryConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2021, 10:46 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
```

```
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
```

```
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
```

```
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryConsoleFullAccess_v2

Descrizione: questa policy fornisce l'accesso completo a tutte le API pubbliche di AWS Elastic Disaster Recovery (AWS DRS), nonché a tutte le API pubbliche di altri AWS servizi utilizzati da AWS DRS Console. Allega questa policy ai tuoi utenti o ruoli.

`AWSElasticDisasterRecoveryConsoleFullAccess_v2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryConsoleFullAccess_v2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2023, 13:35 UTC
- Ora modificata: 18 giugno 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
```

```
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
```

```
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
```

```
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess31",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
```

```
        "arn:aws:ssm:*:*:document/AWSDRS-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSDRS-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSDRS-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSDRS-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSDRS-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSDRS-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSDRS-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSDRS-VerifyTags",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess32",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess33",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess34",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess35",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ConsoleFullAccess36",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess37",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess38",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess39",
      "Effect" : "Allow",
      "Action" : "ec2:CreateFleet",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess40",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess41",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleFullAccess42",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess43",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ConsoleFullAccess44",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryConversionServerPolicy

Descrizione: questa policy è associata al ruolo di istanza del server AWS Elastic Disaster Recovery Conversion. Questa policy consente ai server di conversione Elastic Disaster Recovery (DRS), che sono istanze EC2 lanciate da Elastic Disaster Recovery (DRS), di comunicare con il servizio DRS. Un ruolo IAM con questa policy viene collegato (come profilo di istanza EC2) da DRS ai server di conversione DRS, che vengono avviati e terminati automaticamente da DRS, quando necessario. Non è consigliabile collegare questa policy ai propri utenti o ruoli IAM. I server di conversione DRS vengono utilizzati da Elastic Disaster Recovery quando gli utenti scelgono di ripristinare i server di origine utilizzando la console DRS, la CLI o l'API.

`AWSElasticDisasterRecoveryConversionServerPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryConversionServerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 novembre 2021, 13:42 UTC
- Ora modificata: 27 novembre 2023, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSConversionServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSConversionServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Descrizione: questa policy consente a AWS Elastic Disaster Recovery (DRS) di supportare la replica tra account e il failback tra account.

`AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 maggio 2023, 07:16 UTC
- Ora modificata: 17 gennaio 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeInstances",
        "drs:DescribeSourceServers",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryEc2InstancePolicy

Descrizione: questa policy consente l'installazione e l'utilizzo del AWS Replication Agent, utilizzato da AWS Elastic Disaster Recovery (DRS) per ripristinare i server di origine eseguiti su EC2 (multiregione o Cross-AZ). Un ruolo IAM con questa policy deve essere allegato (come profilo di istanza EC2) alle istanze EC2.

`AWSElasticDisasterRecoveryEc2InstancePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryEc2InstancePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 maggio 2022, 12:30 UTC
- Ora modificata: 27 novembre 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSEc2InstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy5",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryFailbackInstallationPolicy

Descrizione: puoi allegare la AWSElastic DisasterRecoveryFailbackInstallationPolicy policy alle tue identità IAM. Questa policy consente di installare l'Elastic Disaster Recovery Failback Client, che viene utilizzato per eseguire il failback delle istanze di ripristino sull'infrastruttura di origine originale. Allega questa policy agli utenti o ai ruoli IAM di cui fornisci le credenziali durante l'esecuzione dell'Elastic Disaster Recovery Failback Client.

`AWSElasticDisasterRecoveryFailbackInstallationPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryFailbackInstallationPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2021, 11:02 UTC
- Ora modificata: 27 novembre 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource",
        "drs:IssueAgentCertificateForDrs",
        "drs:AssociateFailbackClientToRecoveryInstanceForDrs",
```

```
        "drs:GetSuggestedFailbackClientDeviceMappingForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateFailbackClientDeviceMappingForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryFailbackPolicy

Descrizione: questa policy consente di utilizzare l'Elastic Disaster Recovery Failback Client, utilizzato per ripristinare le istanze di ripristino nell'infrastruttura di origine originale. Ti sconsigliamo di allegare questa policy ai tuoi utenti o ruoli IAM.

`AWSElasticDisasterRecoveryFailbackPolicy`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryFailbackPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica relativa al ruolo del servizio
- Ora di creazione: 17 novembre 2021, 10:41 UTC
- Ora modificata: 22 luglio 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Versione della politica

Versione della politica: v3 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy4",
      "Effect" : "Allow",
```

```
      "Action" : [
        "drs:GetFailbackCommandForDrs",
        "drs:UpdateFailbackClientLastSeenForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyConsistencyAttainedForDrs",
        "drs:GetFailbackLaunchRequestedForDrs",
        "drs:IssueAgentCertificateForDrs",
        "drs:GetAgentSnapshotCreditsForDrs",
        "drs:SendVolumeStatsForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/${aws:SourceIdentity}"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryLaunchActionsPolicy

Descrizione: questa policy consente di utilizzare le autorizzazioni richieste da Amazon SSM e servizi aggiuntivi per eseguire azioni post-lancio in AWS Elastic Disaster Recovery (AWS DRS). Allega questa policy ai tuoi ruoli o utenti IAM.

`AWSElasticDisasterRecoveryLaunchActionsPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryLaunchActionsPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 settembre 2023, 07:38 UTC
- Ora modificata: 18 giugno 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "LaunchActionsPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-*",
        "arn:aws:ssm:*::document/AWSCodeDeployAgent-*",
        "arn:aws:ssm:*::document/AWSConfigRemediation-*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSDisasterRecovery-*",
        "arn:aws:ssm:*::document/AWSDistroOTel-*",
        "arn:aws:ssm:*::document/AWSDocs-*",
        "arn:aws:ssm:*::document/AWSDRS-*",
        "arn:aws:ssm:*::document/AWSEC2-*",
        "arn:aws:ssm:*::document/AWSEC2Launch-*",
        "arn:aws:ssm:*::document/AWSFIS-*",
        "arn:aws:ssm:*::document/AWSFleetManager-*",
        "arn:aws:ssm:*::document/AWSIncidents-*",
        "arn:aws:ssm:*::document/AWSKinesisTap-*",
```

```
        "arn:aws:ssm:*::document/AWSMigration-*",
        "arn:aws:ssm:*::document/AWSNVMe-*",
        "arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
        "arn:aws:ssm:*::document/AWSObservabilityExporter-*",
        "arn:aws:ssm:*::document/AWSPVDriver-*",
        "arn:aws:ssm:*::document/AWSQuickSetupType-*",
        "arn:aws:ssm:*::document/AWSQuickStarts-*",
        "arn:aws:ssm:*::document/AWSRefactorSpaces-*",
        "arn:aws:ssm:*::document/AWSResilienceHub-*",
        "arn:aws:ssm:*::document/AWSSAP-*",
        "arn:aws:ssm:*::document/AWSSAPTools-*",
        "arn:aws:ssm:*::document/AWSSQLServer-*",
        "arn:aws:ssm:*::document/AWSSSO-*",
        "arn:aws:ssm:*::document/AWSSupport-*",
        "arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
        "arn:aws:ssm:*::document/AmazonCloudWatch-*",
        "arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
        "arn:aws:ssm:*::document/AmazonECS-*",
        "arn:aws:ssm:*::document/AmazonEFSUtils-*",
        "arn:aws:ssm:*::document/AmazonEKS-*",
        "arn:aws:ssm:*::document/AmazonInspector-*",
        "arn:aws:ssm:*::document/AmazonInspector2-*",
        "arn:aws:ssm:*::document/AmazonInternal-*",
        "arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
        "arn:aws:ssm:*::document/AwsVssComponents-*",
        "arn:aws:ssm:*::automation-definition/AWS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDistroOTel-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDRS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
        "arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
        "arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
        "arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
        "arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
        "arn:aws:ssm:*::automation-definition/AWSPVDriver-*:*",
```

```
        "arn:aws:ssm:*::automation-definition/AWSQuickSetupType-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickStarts-*:*",
        "arn:aws:ssm:*::automation-definition/AWSRefactorSpaces-*:*",
        "arn:aws:ssm:*::automation-definition/AWSResilienceHub-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAPTools-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSQLServer-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSSO-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSupport-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSystemsManagerSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatch-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatchAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonECS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEFSUtils-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEKS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector2-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInternal-*:*",
        "arn:aws:ssm:*::automation-definition/AwsEnaNetworkDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AwsVssComponents-*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
```

```
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchActionsPolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
```

```
    },
    {
      "Sid" : "LaunchActionsPolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "LaunchActionsPolicy11",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "drs.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryNetworkReplicationPolicy

Descrizione: questa policy consente a AWS Elastic Disaster Recovery (DRS) di supportare la replica di rete.

`AWSElasticDisasterRecoveryNetworkReplicationPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryNetworkReplicationPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 giugno 2023, 12:36 UTC
- Ora modificata: 02 gennaio 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSNetworkReplicationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInstances",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryReadOnlyAccess

Descrizione: puoi allegare la AWSElastic DisasterRecoveryReadOnlyAccess policy alle tue identità IAM. Questa policy fornisce le autorizzazioni a tutti i servizi pubblici in sola lettura APIs di Elastic Disaster Recovery (DRS), nonché ad alcuni altri AWS servizi APIs di sola lettura necessari per utilizzare appieno la console DRS in sola lettura. Collega questa policy ai tuoi utenti o ruoli IAM.

`AWSElasticDisasterRecoveryReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2021, 10:50 UTC
- Ora modificata: 29 luglio 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess4",
```

```
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess5",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommandInvocations",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess6",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameter",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
    },
    {
      "Sid" : "DRSReadOnlyAccess7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-CreateImage",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ]
    },
    {
      "Sid" : "DRSReadOnlyAccess8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryRecoveryInstancePolicy

Descrizione: questa policy è associata al ruolo di istanza dell'istanza di ripristino di Elastic Disaster Recovery. Questa policy consente all'istanza di ripristino Elastic Disaster Recovery (DRS), che sono istanze EC2 lanciate da Elastic Disaster Recovery, di comunicare con il servizio DRS e di effettuare il failback sull'infrastruttura di origine originale. Un ruolo IAM con questa policy è associato (come profilo di istanza EC2) da Elastic Disaster Recovery alle istanze di ripristino DRS. Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

`AWSElasticDisasterRecoveryRecoveryInstancePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryRecoveryInstancePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 novembre 2021, 10:20 UTC
- Ora modificata: 27 novembre 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSRecoveryInstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:UpdateReplicationCertificateForDrs",
        "drs:NotifyReplicationServerAuthenticationForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*",
      "Condition" : {
        "StringEquals" : {
          "drs:EC2InstanceARN" : "${ec2:SourceInstanceARN}"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeRecoveryInstances"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy5",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
```

```
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryReplicationServerPolicy

Descrizione: questa policy è associata al ruolo di istanza del server Elastic Disaster Recovery Replication. Questa policy consente ai server di replica Elastic Disaster Recovery (DRS), che sono istanze EC2 lanciate da Elastic Disaster Recovery (DRS), di comunicare con il servizio DRS e di

creare istantanee EBS nel tuo. Account AWS Un ruolo IAM con questa policy è associato (come profilo di istanza EC2) da Elastic Disaster Recovery ai server di replica DRS, che vengono avviati e terminati automaticamente da DRS, in base alle esigenze. I server di replica DRS vengono utilizzati per facilitare la replica dei dati dai server esterni a AWS, come parte del processo di ripristino gestito da DRS. Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

`AWSElasticDisasterRecoveryReplicationServerPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryReplicationServerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 novembre 2021, 13:34 UTC
- Ora modificata: 27 novembre 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReplicationServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
```

```
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentSnapshotCreditsForDrs",
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeSnapshotRequestsForDrs",
        "drs:BatchDeleteSnapshotRequestForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:BatchCreateVolumeSnapshotGroupForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyVolumeEventForDrs",
        "drs:SendVolumeStatsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy5",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryServiceRolePolicy

Descrizione: questa policy consente a Elastic Disaster Recovery di gestire AWS le risorse per tuo conto.

`AWSElasticDisasterRecoveryServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 novembre 2021, 10:56 UTC
- Ora modificata: 5 gennaio 2025, 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "DRSServiceRolePolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy12",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "DRSServiceRolePolicy15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy16",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "DRSServiceRolePolicy22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy25",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryReplicationServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
```

```
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy28",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy29",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy31",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
```

```
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy32",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy33",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryStagingAccountPolicy

Descrizione: questa policy consente l'accesso in sola lettura alle risorse AWS Elastic Disaster Recovery (DRS) come server di origine e job. Consente inoltre di creare un'istantanea convertita e di condividerla con un account specifico.

`AWSElasticDisasterRecoveryStagingAccountPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryStagingAccountPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 maggio 2022, 09:49 UTC
- Ora modificata: 27 novembre 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Descrizione: questa policy viene utilizzata da AWS Elastic Disaster Recovery (DRS) per ripristinare i server di origine in un account di destinazione separato e per consentire il failback. Non è consigliabile collegare questa policy agli utenti o ai ruoli IAM.

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 gennaio 2023, 12:11 UTC
- Ora modificata: 27 novembre 2023, 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicyv21",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicyv22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSStagingAccountPolicyv23",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : [
        "arn:aws:drs:*:*:source-server/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticLoadBalancingClassicServiceRolePolicy

Descrizione: Policy Service Linked Role per AWS Elastic Load Balancing Control Plane - Classic

`AWSElasticLoadBalancingClassicServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 settembre 2017, 22:36 UTC
- Ora modificata: 07 ottobre 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
```

```
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElasticLoadBalancingServiceRolePolicy

Descrizione: policy Service Linked Role per AWS Elastic Load Balancing Control Plane

`AWSElasticLoadBalancingServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 settembre 2017, 22:19 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:ReleaseAddress",
        "ec2:UnassignIpv6Addresses",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "ec2:AllocateIpamPoolCidr",
        "logs:CreateLogDelivery",
```

```
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaConnectCreateBridge

Descrizione: fornisce l'accesso completo per creare MediaConnect Gateway Bridges e tutte le relative risorse secondarie associate.

`AWSElementalMediaConnectCreateBridge`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaConnectCreateBridge` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 marzo 2026, 16:57 UTC
- Ora modificata: 19 marzo 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectCreateBridge`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:CreateBridge",
        "mediaconnect:AddBridgeSources",
        "mediaconnect:AddBridgeOutputs"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:bridge:*:*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeSource/*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeOutput/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaConnectCreateFlow

Descrizione: fornisce l'accesso completo alla creazione di MediaConnect Flows e a tutte le relative risorse secondarie associate.

`AWSElementalMediaConnectCreateFlow`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaConnectCreateFlow` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 marzo 2026, 16:57 UTC
- Ora modificata: 19 marzo 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectCreateFlow`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "mediaconnect.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:CreateFlow",
        "mediaconnect:AddFlowSources",
        "mediaconnect:AddFlowOutputs",
```

```
        "mediaconnect:GrantFlowEntitlements",
        "mediaconnect:AddFlowMediaStreams",
        "mediaconnect:AddFlowVpcInterfaces",
        "mediaconnect:TagResource"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:flow:*:*",
        "arn:aws:mediaconnect:*:*:source:*:*",
        "arn:aws:mediaconnect:*:*:output:*:*",
        "arn:aws:mediaconnect:*:*:entitlement:*:*",
        "arn:aws:mediaconnect:*:*:flow:*:*/vpcInterface/*",
        "arn:aws:mediaconnect:*:*:flow:*:*/mediaStream/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaConnectDeleteBridge

Descrizione: fornisce l'accesso completo per eliminare MediaConnect Gateway Bridges e tutte le relative risorse secondarie associate.

`AWSElementalMediaConnectDeleteBridge`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaConnectDeleteBridge` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 19 marzo 2026, 19:57 UTC
- Ora modificata: 19 marzo 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectDeleteBridge`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DeleteBridge",
        "mediaconnect:RemoveBridgeSource",
        "mediaconnect:RemoveBridgeOutput"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:bridge:*:*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeSource/*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeOutput/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaConnectDeleteFlow

Descrizione: fornisce l'accesso completo all'eliminazione di MediaConnect Flows e a tutte le relative risorse secondarie associate.

`AWSElementalMediaConnectDeleteFlow`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaConnectDeleteFlow` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 marzo 2026, 19:57 UTC
- Ora modificata: 19 marzo 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectDeleteFlow`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DeleteFlow",
```

```
        "mediaconnect:RemoveFlowSource",
        "mediaconnect:RemoveFlowOutput",
        "mediaconnect:RevokeFlowEntitlement",
        "mediaconnect:RemoveFlowMediaStream",
        "mediaconnect:RemoveFlowVpcInterface"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:flow:*:*",
        "arn:aws:mediaconnect:*:*:source:*:*",
        "arn:aws:mediaconnect:*:*:output:*:*",
        "arn:aws:mediaconnect:*:*:entitlement:*:*",
        "arn:aws:mediaconnect:*:*:flow:*:*/vpcInterface/*",
        "arn:aws:mediaconnect:*:*:flow:*:*/mediaStream/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaConnectFullAccess

Descrizione: fornisce l'accesso completo alle MediaConnect risorse AWS elementali.

`AWSElementalMediaConnectFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaConnectFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 febbraio 2025, 20:07 UTC

- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaConnectReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle risorse AWS MediaConnect Elemental.

`AWSElementalMediaConnectReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaConnectReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 febbraio 2025, 20:07 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:ListBridges",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGatewayInstances",
        "mediaconnect:ListGateways",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeFlowSourceMetadata",
        "mediaconnect:DescribeFlowSourceThumbnail",
        "mediaconnect:DescribeGateway",
```

```
        "mediaconnect:DescribeGatewayInstance",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaConvertFullAccess

Descrizione: fornisce l'accesso completo a AWS Elemental MediaConvert tramite l'SDK Console di gestione AWS and.

`AWSElementalMediaConvertFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaConvertFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 giugno 2018, 19:25 UTC
- Ora modificata: 10 giugno 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "mediaconvert.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaConvertReadOnly

Descrizione: fornisce l'accesso in sola lettura a AWS Elemental MediaConvert tramite l'SDK Console di gestione AWS and.

`AWSElementalMediaConvertReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaConvertReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 giugno 2018, 19:25 UTC
- Ora modificata: 10 giugno 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaLiveFullAccess

Descrizione: fornisce l'accesso completo alle risorse AWS elementali MediaLive

`AWSElementalMediaLiveFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaLiveFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 luglio 2020, 17:07 UTC
- Ora modificata: 08 luglio 2020, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "medialive:*",
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaLiveReadOnly

Descrizione: fornisce l'accesso in sola lettura alle AWS risorse elementali MediaLive

`AWSElementalMediaLiveReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaLiveReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 luglio 2020, 16:38 UTC
- Ora modificata: 22 luglio 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSElementalMediaLiveReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "medialive:Get*",
        "medialive:List*",
        "medialive:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaPackageFullAccess

Descrizione: fornisce l'accesso completo alle risorse AWS elementali MediaPackage

`AWSElementalMediaPackageFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaPackageFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 dicembre 2017, 23:39 UTC
- Ora modificata: 29 dicembre 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackage:*",
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaPackageReadOnly

Descrizione: fornisce l'accesso in sola lettura alle AWS risorse elementali MediaPackage

`AWSElementalMediaPackageReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaPackageReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 dicembre 2017, 00:04 UTC
- Ora modificata: 30 dicembre 2017, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackage:List*",
      "mediapackage:Describe*"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaPackageV2FullAccess

Descrizione: fornisce l'accesso completo alle risorse AWS Elemental MediaPackage V2.

`AWSElementalMediaPackageV2FullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaPackageV2FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 luglio 2023, 20:29 UTC
- Ora modificata: 25 luglio 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaPackageV2ReadOnly

Descrizione: fornisce accesso in sola lettura alle risorse AWS MediaPackage Elemental V2.

`AWSElementalMediaPackageV2ReadOnly`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaPackageV2ReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 luglio 2023, 20:31 UTC
- Ora modificata: 25 luglio 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaStoreFullAccess

Descrizione: fornisce accesso completo in lettura e scrittura a tutti MediaStore APIs

`AWSElementalMediaStoreFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaStoreFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 marzo 2018, 23:15 UTC
- Ora modificata: 5 marzo 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaStoreReadOnly

Descrizione: fornisce autorizzazioni di sola lettura per MediaStore APIs

`AWSElementalMediaStoreReadOnly`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaStoreReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 8 marzo 2018, 19:48 UTC
- Ora modificata: 08 marzo 2018, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaTailorFullAccess

Descrizione: fornisce l'accesso completo alle risorse AWS elementali MediaTailor

`AWSElementalMediaTailorFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaTailorFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 novembre 2021, 00:04 UTC
- Ora modificata: 23 novembre 2021, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
```

```
    "Effect" : "Allow",
    "Action" : "mediatailor:*",
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSElementalMediaTailorReadOnly

Descrizione: fornisce l'accesso in sola lettura alle AWS risorse elementali MediaTailor

`AWSElementalMediaTailorReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSElementalMediaTailorReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 novembre 2021, 00:05 UTC
- Ora modificata: 23 novembre 2021, 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediatailor:List*",
      "mediatailor:Describe*",
      "mediatailor:Get*"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEnhancedClassicNetworkingMangementPolicy

Descrizione: Politica per abilitare la funzionalità classica avanzata di gestione della rete.

`AWSEnhancedClassicNetworkingMangementPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 settembre 2017, 17:29 UTC

- Ora modificata: 20 settembre 2017, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEntityResolutionConsoleFullAccess

Descrizione: fornisce l'accesso completo da console a AWS Entity Resolution e ai servizi correlati.

`AWSEntityResolutionConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSEntityResolutionConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 agosto 2023, 17:54 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetSchema",
        "glue:SearchTables",
        "glue:GetSchemaByDefinition",
```

```
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketsConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3SourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TaggingConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
```

```
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesToPickRoleForPassing",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEntityResolutionService",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*entityresolution*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "entityresolution.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/entity-resolution-automatic*"
      ]
    },
    {
      "Sid" : "ADXReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:ListInstances",
        "profile:ListDomains",
        "profile:GetDomain",
        "profile:ListIntegrations",
        "profile:ListAccountIntegrations",
        "profile:ListProfileObjectTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "profile:PutProfileObjectType"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/*/object-types/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSEntityResolutionConsoleReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS Entity Resolution tramite. Console di gestione AWS

`AWSEntityResolutionConsoleReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSEntityResolutionConsoleReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 agosto 2023, 18:18 UTC
- Ora modificata: 17 agosto 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionRead",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:Get*",
        "entityresolution:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSFaultInjectionSimulatorEC2Access

Descrizione: questa policy concede l'autorizzazione al servizio Fault Injection Simulator in EC2 e ad altri servizi necessari per eseguire azioni FIS.

`AWSFaultInjectionSimulatorEC2Access`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSFaultInjectionSimulatorEC2Access` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 ottobre 2022, 20:39 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEc2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:SendSpotInstanceInterruptions",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "AllowEc2InstancesWithEncryptedEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
```

```
      "Sid" : "AllowSSMStopOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:ListCommands"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSFaultInjectionSimulatorECSAccess

Descrizione: questa policy concede l'autorizzazione al servizio Fault Injection Simulator in ECS e ad altri servizi necessari per eseguire azioni FIS.

`AWSFaultInjectionSimulatorECSAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSFaultInjectionSimulatorECSAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 ottobre 2022, 20:37 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Clusters",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:ListContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "Tasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks",
        "ecs:StopTask"
      ],
      "Resource" : [
```

```
        "arn:aws:ecs:*:*:task/*/*"
      ]
    },
    {
      "Sid" : "ContainerInstances",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    },
    {
      "Sid" : "ListTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSend",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "SSMList",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeContainerInstances",
      "Effect" : "Allow",
      "Action" : "ecs:DescribeContainerInstances",
      "Resource" : "arn:aws:ecs:*:*:container-instance/*/*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSFaultInjectionSimulatorEKSAccess

Descrizione: questa politica concede l'autorizzazione al servizio Fault Injection Simulator in EKS e ad altri servizi necessari per eseguire le azioni FIS.

`AWSFaultInjectionSimulatorEKSAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSFaultInjectionSimulatorEKSAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 ottobre 2022, 20:34 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeSubnets",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DescribeNodeGroup",
      "Effect" : "Allow",
      "Action" : "eks:DescribeNodegroup",
      "Resource" : "arn:aws:eks:*:*:nodegroup/*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSFaultInjectionSimulatorNetworkAccess

Descrizione: questa policy concede al servizio Fault Injection Simulator l'autorizzazione per le reti EC2 e altri servizi necessari per eseguire azioni FIS.

`AWSFaultInjectionSimulatorNetworkAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSFaultInjectionSimulatorNetworkAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 ottobre 2022, 20:32 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTagsOnNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAcl",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkAcl",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAclOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "VpcActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReplaceNetworkAclAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceNetworkAclAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*"
      ]
    },
    {
      "Sid" : "GetManagedPrefixListEntries",
      "Effect" : "Allow",
      "Action" : "ec2:GetManagedPrefixListEntries",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*"
    },
    {
      "Sid" : "CreateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateTagsOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateManagedPrefixList",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRoute",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceOnSubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DeleteNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateManagedPrefixList",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ReplaceRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceRouteTableAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:AssociateRouteTable",
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "DisassociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DisassociateRouteTableOnSubnet",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "ModifyVpcEndpointOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoint",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ]
    },
    {
      "Sid" : "TransitGatewayRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:AssociateTransitGatewayRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSFaultInjectionSimulatorRDSAccess

Descrizione: questa politica concede al servizio Fault Injection Simulator l'autorizzazione a utilizzare RDS e altri servizi necessari per eseguire azioni FIS.

`AWSFaultInjectionSimulatorRDSAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSFaultInjectionSimulatorRDSAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 26 ottobre 2022, 20:30 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFailover",
      "Effect" : "Allow",
      "Action" : [
        "rds:FailoverDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AllowReboot",
      "Effect" : "Allow",
      "Action" : [
        "rds:RebootDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "DescribeResources",
```

```
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSFaultInjectionSimulatorSSMAccess

Descrizione: questa politica concede al servizio Fault Injection Simulator l'autorizzazione in SSM e altri servizi necessari per eseguire azioni FIS.

`AWSFaultInjectionSimulatorSSMAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSFaultInjectionSimulatorSSMAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 26 ottobre 2022, 15:33 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSFinSpaceServiceRolePolicy

Descrizione: Politica per consentire l'accesso Servizio AWS e le risorse utilizzate o gestite da Amazon FinSpace

`AWSFinSpaceServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 maggio 2023, 16:42 UTC
- Ora modificata: 01 dicembre 2023, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSFinSpaceServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/FinSpace",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSFMAdminFullAccess

Descrizione: accesso completo per AWS FM Administrator

`AWSFMAdminFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSFMAdminFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 maggio 2018, 18:06 UTC
- Ora modificata: 20 ottobre 2022, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:*",
        "waf:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:PutLoggingConfiguration",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fms.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSFMAdminReadOnlyAccess

Descrizione: accesso in sola lettura per AWS FM Administrator che consente il monitoraggio delle operazioni AWS FM

`AWSFMAdminReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSFMAdminReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 maggio 2018, 20:07 UTC
- Ora modificata: 31 ottobre 2022, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:Get*",
        "fms:List*",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListChildren",
```

```
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSFMMemberReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle azioni AWS WAF per gli account membri di AWS Firewall Manager

`AWSFMMemberReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSFMMemberReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 maggio 2018, 21:05 UTC
- Ora modificata: 09 maggio 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSForWordPressPluginPolicy

Descrizione: politica gestita AWS per il plugin For Wordpress

`AWSForWordPressPluginPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSForWordPressPluginPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 ottobre 2019, 00:27 UTC
- Ora modificata: 20 gennaio 2020, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Permissions1",
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech",
        "polly:DescribeVoices",
        "translate:TranslateText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Permissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::audio_for_wordpress*",
        "arn:aws:s3:::audio-for-wordpress*"
      ]
    },
    {
      "Sid" : "Permissions3",
      "Effect" : "Allow",
```

```
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DescribeCertificate",
        "acm:RequestCertificate",
        "cloudformation:CreateStack",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "Permissions4",
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:UpdateStack",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetDistribution",
        "cloudfront:GetInvalidation",
        "cloudfront:TagResource",
        "cloudfront:UpdateDistribution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGitSyncServiceRolePolicy

Descrizione: Policy che consente a AWS Code Connections di sincronizzare i contenuti dal tuo repository git

`AWSGitSyncServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 16 novembre 2023, 17:05 UTC
- Ora modificata: 26 aprile 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGlobalAcceleratorSLRPolicy

Descrizione: Politica di concessione delle autorizzazioni a AWS Global Accelerator per gestire le interfacce di rete elastiche e i gruppi di sicurezza EC2.

`AWSGlobalAcceleratorSLRPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 5 aprile 2019, 19:39 UTC
- Ora modificata: 29 ottobre 2024, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
        }
      }
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGlueConsoleFullAccess

Descrizione: Fornisce l'accesso completo a AWS Glue tramite Console di gestione AWS

`AWSGlueConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSGlueConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 agosto 2017, 13:37 UTC
- Ora modificata: 14 luglio 2023, 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAppPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:DescribeRecipe"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
```

```
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGlueConsoleSageMakerNotebookFullAccess

Descrizione: Fornisce l'accesso completo a AWS Glue tramite Console di gestione AWS e l'accesso alle istanze del notebook sagemaker.

`AWSGlueConsoleSageMakerNotebookFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSGlueConsoleSageMakerNotebookFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 ottobre 2018, 17:52 UTC
- Ora modificata: 15 luglio 2021, 15:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "rds:DescribeDBInstances",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "sagemaker:ListNotebookInstances",
        "cloudformation:ListStacks",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
```

```
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/aws-glue-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/aws-glue-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AwsGlueDataBrewFullAccessPolicy

Descrizione: Fornisce l'accesso completo a AWS Glue DataBrew tramite Console di gestione AWS. Fornisce inoltre un accesso selezionato ai servizi correlati (ad esempio, S3, KMS, Glue).

`AwsGlueDataBrewFullAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AwsGlueDataBrewFullAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 novembre 2020, 16:51 UTC
- Ora modificata: 04 febbraio 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "databrew:CreateDataset",
        "databrew:DescribeDataset",
        "databrew:ListDatasets",
        "databrew:UpdateDataset",
        "databrew:DeleteDataset",
        "databrew:CreateProject",
        "databrew:DescribeProject",
        "databrew:ListProjects",
        "databrew:StartProjectSession",
        "databrew:SendProjectSessionAction",
        "databrew:UpdateProject",
        "databrew:DeleteProject",
        "databrew:CreateRecipe",
        "databrew:DescribeRecipe",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:PublishRecipe",
        "databrew:UpdateRecipe",
        "databrew:BatchDeleteRecipeVersion",
        "databrew:DeleteRecipeVersion",
        "databrew:CreateRecipeJob",
        "databrew:CreateProfileJob",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:StartJobRun",
        "databrew:StopJobRun",
        "databrew:UpdateProfileJob",
        "databrew:UpdateRecipeJob",
        "databrew:DeleteJob",
        "databrew:CreateSchedule",
        "databrew:DescribeSchedule",
        "databrew:ListSchedules",
        "databrew:UpdateSchedule",
        "databrew:DeleteSchedule",
        "databrew:CreateRuleset",
        "databrew:DeleteRuleset",
        "databrew:DescribeRuleset",
        "databrew:ListRulesets",
```

```
        "databrew:UpdateRuleset",
        "databrew:ListTagsForResource",
        "databrew:TagResource",
        "databrew:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetDataCatalogEncryptionSettings",
        "dataexchange:ListDataSets",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListRevisionAssets",
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:GetJob",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
```

```
        "s3:GetLifecycleConfiguration",
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "sts:GetCallerIdentity",
        "cloudtrail:LookupEvents",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AwsGlueDataBrew-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*/awsgluedatabrew*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AwsGlueDataBrew-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateRandom"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "databrew!default"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGlueDataBrewServiceRole

Descrizione: questa politica concede il permesso a glue di eseguire azioni sul catalogo dati Glue dell'utente, questa politica fornisce anche l'autorizzazione alle azioni ec2 per consentire a glue di creare ENI per connettersi alle risorse nel VPC, inoltre consentire a glue di accedere ai dati registrati in lakeformation e il permesso di accedere al cloudwatch dell'utente

`AWSGlueDataBrewServiceRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSGlueDataBrewServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 04 dicembre 2020, 21:26 UTC
- Ora modificata: 20 marzo 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetConnection"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePIIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGetCustomEntityTypes",
        "glue:GetCustomEntityType"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3PublicDatasetAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Sid" : "EC2NetworkingPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws-glue-service-resource" : "*"
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2GlueTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
```

```
      ]
    },
    {
      "Sid" : "GlueDatabrewLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
      ]
    },
    {
      "Sid" : "LakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGlueSchemaRegistryFullAccess

Descrizione: Fornisce l'accesso completo al servizio AWS Glue Schema Registry

`AWSGlueSchemaRegistryFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSGlueSchemaRegistryFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2020, 00:19 UTC
- Ora modificata: 20 novembre 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateRegistry",
        "glue:UpdateRegistry",
        "glue:DeleteRegistry",
        "glue:GetRegistry",
        "glue:ListRegistries",
```

```
        "glue:CreateSchema",
        "glue:UpdateSchema",
        "glue:DeleteSchema",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:RegisterSchemaVersion",
        "glue:DeleteSchemaVersions",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:ListSchemaVersions",
        "glue:CheckSchemaVersionValidity",
        "glue:PutSchemaVersionMetadata",
        "glue:RemoveSchemaVersionMetadata",
        "glue:QuerySchemaVersionMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSGlueSchemaRegistryTagsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
        "glue:TagResource",
        "glue:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:schema/*",
        "arn:aws:glue:*:*:registry/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGlueSchemaRegistryReadonlyAccess

Descrizione: fornisce l'accesso in sola lettura al servizio AWS Glue Schema Registry

`AWSGlueSchemaRegistryReadonlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSGlueSchemaRegistryReadonlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2020, 00:20 UTC
- Ora modificata: 20 novembre 2020, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryReadonlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:GetSchemaByDefinition",
```

```
        "glue:GetSchemaVersion",
        "glue:ListSchemaVersions",
        "glue:GetSchemaVersionsDiff",
        "glue:CheckSchemaVersionValidity",
        "glue:QuerySchemaVersionMetadata",
        "glue:GetTags"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGlueServiceNotebookRole

Descrizione: ruolo del servizio Policy for AWS Glue che consente al cliente di gestire il server notebook

`AWSGlueServiceNotebookRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSGlueServiceNotebookRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 13:37 UTC
- Ora modificata: 09 ottobre 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeleteDatabase",
        "glue:DeletePartition",
        "glue:DeleteTable",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:CreateConnection",
        "glue:CreateJob",
        "glue:DeleteConnection",
        "glue:DeleteJob",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:UpdateJob",
```

```
        "glue:BatchDeleteConnection",
        "glue:UpdateConnection",
        "glue:GetUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:DeleteUserDefinedFunction",
        "glue:CreateUserDefinedFunction",
        "glue:BatchGetPartition",
        "glue:BatchDeletePartition",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteTable",
        "glue:UpdateDevEndpoint",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGlueServiceRole

Descrizione: ruolo del servizio Policy for AWS Glue che consente l'accesso a servizi correlati tra cui EC2, S3 e Cloudwatch Logs

`AWSGlueServiceRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSGlueServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 13:37 UTC
- Ora modificata: 11 settembre 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
```

```
        "arn:aws:logs:*:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AwsGlueSessionUserRestrictedNotebookPolicy

Descrizione: fornisce autorizzazioni che consentono agli utenti di creare e utilizzare solo le sessioni di notebook associate all'utente. Questa politica include anche le autorizzazioni per consentire esplicitamente agli utenti di passare un ruolo di sessione Glue limitato.

`AwsGlueSessionUserRestrictedNotebookPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AwsGlueSessionUserRestrictedNotebookPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 aprile 2022, 15:24 UTC
- Ora modificata: 15 agosto 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions1",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "NotebookAllowActions2",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions3",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "NotebookDenyActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "NotebookPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/service-role/
AwsGlueSessionServiceRoleUserRestrictedForNotebook*",
        "arn:aws:iam::*:role/AwsGlueSessionUserRestrictedNotebookServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AwsGlueSessionUserRestrictedNotebookServiceRole

Descrizione: Fornisce l'accesso completo a tutte le risorse AWS Glue ad eccezione delle sessioni. Permette agli utenti di creare e utilizzare solo le sessioni notebook associate all'utente. Questa politica include anche altre autorizzazioni necessarie a AWS Glue per gestire le risorse Glue in altri AWS servizi.

`AwsGlueSessionUserRestrictedNotebookServiceRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AwsGlueSessionUserRestrictedNotebookServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 18 aprile 2022, 15:27 UTC
- Ora modificata: 15 agosto 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AwsGlueSessionUserRestrictedPolicy

Descrizione: fornisce autorizzazioni che consentono agli utenti di creare e utilizzare solo le sessioni interattive associate all'utente. Questa politica include anche le autorizzazioni per consentire esplicitamente agli utenti di passare un ruolo di sessione Glue limitato.

`AwsGlueSessionUserRestrictedPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AwsGlueSessionUserRestrictedPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 aprile 2022, 21:31 UTC
- Ora modificata: 5 agosto 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
```

```
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessions",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
```

```
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AwsGlueSessionUserRestrictedServiceRole

Descrizione: Fornisce l'accesso completo a tutte le risorse AWS Glue ad eccezione delle sessioni. Permette agli utenti di creare e utilizzare solo le sessioni interattive associate all'utente. Questa politica include anche altre autorizzazioni necessarie a AWS Glue per gestire le risorse Glue in altri AWS servizi.

`AwsGlueSessionUserRestrictedServiceRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AwsGlueSessionUserRestrictedServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 aprile 2022, 21:30 UTC
- Ora modificata: 5 agosto 2024, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowStatementActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessionsAction",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectCrawlerActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Sid" : "AllowLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Sid" : "AllowTagsActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGrafanaAccountAdministrator

Descrizione: fornisce l'accesso all'interno di Amazon Grafana per creare e gestire aree di lavoro per l'intera organizzazione.

`AWSGrafanaAccountAdministrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSGrafanaAccountAdministrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 febbraio 2021, 00:20 UTC
- Ora modificata: 15 febbraio 2022, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaOrganizationAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMGetRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "grafana.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGrafanaConsoleReadOnlyAccess

Descrizione: accesso alle operazioni di sola lettura in Amazon Grafana.

`AWSGrafanaConsoleReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSGrafanaConsoleReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 febbraio 2021, 00:10 UTC
- Ora modificata: 15 febbraio 2022, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaConsoleReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:Describe*",
        "grafana:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGrafanaWorkspacePermissionManagement

Descrizione: offre solo la possibilità di aggiornare le autorizzazioni utente e di gruppo per le aree di lavoro AWS Grafana.

`AWSGrafanaWorkspacePermissionManagement`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSGrafanaWorkspacePermissionManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 febbraio 2021, 00:15 UTC
- Ora modificata: 15 marzo 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGrafanaWorkspacePermissionManagementV2

Descrizione: offre la possibilità di aggiornare le autorizzazioni di utenti e gruppi di IAM Identity Center (iDC) per le aree di lavoro Amazon Managed Grafana.

`AWSGrafanaWorkspacePermissionManagementV2`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSGrafanaWorkspacePermissionManagementV2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 gennaio 2024, 18:39 UTC
- Ora modificata: 5 gennaio 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGreengrassFullAccess

Descrizione: questa politica offre pieno accesso alle azioni di configurazione, gestione e implementazione di AWS Greengrass

`AWSGreengrassFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSGreengrassFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 maggio 2017, 00:47 UTC
- Ora modificata: 03 maggio 2017, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGreengrassReadOnlyAccess

Descrizione: questa policy consente l'accesso in sola lettura alle azioni di configurazione, gestione e implementazione di AWS Greengrass

`AWSGreengrassReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSGreengrassReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 ottobre 2018, 16:01 UTC
- Ora modificata: 30 ottobre 2018, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:List*",
        "greengrass:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGreengrassResourceAccessRolePolicy

Descrizione: ruolo del servizio Policy for AWS Greengrass che consente l'accesso a servizi correlati, tra cui i thing shadow AWS Lambda e AWS IoT.

`AWSGreengrassResourceAccessRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSGreengrassResourceAccessRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 febbraio 2017, 21:17 UTC

- Ora modificata: 14 novembre 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGreengrassAccessToShadows",
      "Action" : [
        "iot:DeleteThingShadow",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iot:*:*:thing/GG_*",
        "arn:aws:iot:*:*:thing/*-gcm",
        "arn:aws:iot:*:*:thing/*-gda",
        "arn:aws:iot:*:*:thing/*-gci"
      ]
    },
    {
      "Sid" : "AllowGreengrassToDescribeThings",
      "Action" : [
        "iot:DescribeThing"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:thing/*"
    },
    {
```

```
      "Sid" : "AllowGreengrassToDescribeCertificates",
      "Action" : [
        "iot:DescribeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:cert/*"
    },
    {
      "Sid" : "AllowGreengrassToCallGreengrassServices",
      "Action" : [
        "greengrass:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetLambdaFunctions",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetGreengrassSecrets",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Sid" : "AllowGreengrassAccessToS3Objects",
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::*Greengrass*",
        "arn:aws:s3:::*GreenGrass*",
        "arn:aws:s3:::*greengrass*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*SageMaker*",
```

```
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowGreengrassAccessToS3BucketLocation",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassAccessToSageMakerTrainingJobs",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSGroundStationAgentInstancePolicy

Descrizione: fornisce all'istanza Dataflow Endpoint le autorizzazioni per utilizzare l'agente Ground Station AWS

`AWSGroundStationAgentInstancePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSGroundStationAgentInstancePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 marzo 2023, 15:23 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "groundstation:RegisterAgent",
        "groundstation:UpdateAgentStatus",
        "groundstation:GetAgentConfiguration",
        "groundstation:GetAgentTaskResponseUrl"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSHealth_EventProcessorServiceRolePolicy

Descrizione: consente a AWS Health di abilitare la funzionalità Health Event Processor.

`AWSHealth_EventProcessorServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 13 gennaio 2023, 19:24 UTC
- Ora modificata: 13 gennaio 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "event-processor.health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSHealthFullAccess

Descrizione: consente l'accesso completo alle API e alle notifiche AWS Health e alla Personal Health Dashboard

`AWSHealthFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSHealthFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 dicembre 2016, 12:30 UTC
- Ora modificata: 16 novembre 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "health:*",
        "organizations:ListAccounts",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "health.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSHealthImagingFullAccess

Descrizione: Fornisce l'accesso completo al servizio AWS Health Imaging.

`AWSHealthImagingFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSHealthImagingFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 luglio 2023, 23:39 UTC
- Ora modificata: 25 luglio 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "medical-imaging.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSHealthImagingReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura al servizio AWS Health Imaging.

`AWSHealthImagingReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSHealthImagingReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 luglio 2023, 23:40 UTC
- Ora modificata: 01 agosto 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:GetDICOMImportJob",
        "medical-imaging:GetDatastore",
        "medical-imaging:GetImageFrame",
        "medical-imaging:GetImageSet",
        "medical-imaging:GetImageSetMetadata",
        "medical-imaging:ListDICOMImportJobs",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListImageSetVersions",
        "medical-imaging:ListTagsForResource",
        "medical-imaging:SearchImageSets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSHealthImagingServiceRolePolicy

Descrizione: fornisce le autorizzazioni per AWS HealthImaging gestire le operazioni di servizio e pubblicare le metriche del servizio

`AWSHealthImagingServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 30 gennaio 2026, 18:34 UTC
- Ora modificata: 30 gennaio 2026, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealthImagingServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/HealthImaging"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSHealthOmicsServiceLinkedRolePolicy

Descrizione: Policy gestita per il ruolo collegato ad Amazon HealthOmics Service

`AWSHealthOmicsServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 4 marzo 2026, 22:57 UTC
- Ora modificata: 4 marzo 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealthOmicsServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEC2DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowVpcGetActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "AllowCreateNetworkInterfaceWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Service" : "HealthOmics"
        }
      }
    },
    {
      "Sid" : "AllowCreateNetworkInterfaceSubnetSecurityGroup",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowCreateTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "AllowDeleteNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "HealthOmics"
        }
      }
    },
    {
      "Sid" : "AllowAssignUnassignPrivateIpAddresses",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "HealthOmics"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIAMIdentityCenterAllowListForIdentityContext

Descrizione: fornisce l'elenco delle azioni consentite per i ruoli assunti con il contesto di identità IAM Identity Center. AWS Security Token Service (AWS STS) associa automaticamente questa policy ai ruoli presunti. Il contesto di identità viene passato come ProvidedContext.

`AWSIAMIdentityCenterAllowListForIdentityContext`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIAMIdentityCenterAllowListForIdentityContext` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 novembre 2023, 15:21 UTC
- Ora modificata: 1 ottobre 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "aoss:APIAccessAll",
```

```
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:ListSteps",
        "es:ESHttpHead",
        "es:ESHttpPost",
        "es:ESHttpGet",
        "es:ESHttpPatch",
        "es:ESHttpDelete",
        "es:ESHttpPut",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
```

```
        "glue:GetTableVersions",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:SearchTables",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchUpdatePartition",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "lakeformation:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "qapps:CreateQApp",
        "qapps:PredictProblemStatementFromConversation",
        "qapps:PredictQAppFromProblemStatement",
        "qapps:CopyQApp",
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:UpdateQApp",
        "qapps:DeleteQApp",
```

```
        "qapps:AssociateQAppWithUser",
        "qapps:DisassociateQAppFromUser",
        "qapps:ImportDocumentToQApp",
        "qapps:ImportDocumentToQAppSession",
        "qapps:CreateLibraryItem",
        "qapps:GetLibraryItem",
        "qapps:UpdateLibraryItem",
        "qapps:CreateLibraryItemReview",
        "qapps:ListLibraryItems",
        "qapps:CreateSubscriptionToken",
        "qapps:StartQAppSession",
        "qapps:StopQAppSession",
        "qapps:PredictQApp",
        "qapps:ImportDocument",
        "qapps:AssociateLibraryItemReview",
        "qapps:DisassociateLibraryItemReview",
        "qapps:GetQAppSession",
        "qapps:UpdateQAppSession",
        "qapps:GetQAppSessionMetadata",
        "qapps:UpdateQAppSessionMetadata",
        "qapps:TagResource",
        "qapps:ListQAppSessionData",
        "qapps:ExportQAppSessionData",
        "qbusiness:Chat",
        "qbusiness:ChatSync",
        "qbusiness:ListConversations",
        "qbusiness:ListMessages",
        "qbusiness:DeleteConversation",
        "qbusiness:PutFeedback",
        "sts:SetContext"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIAMRoleManagerServiceRolePolicy

Descrizione: consente a IAM Role Manager di gestire le risorse del tuo account per tuo conto.

`AWSIAMRoleManagerServiceRolePolicy`è una policy AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 15 luglio 2026, 23:57 UTC
- Ora modificata: 15 luglio 2026, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIAMRoleManagerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageServiceLinkedAnalyzer",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CreateServiceLinkedAnalyzer",
        "access-analyzer:DeleteServiceLinkedAnalyzer"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIdentityCenterExternalManagementPolicy

Descrizione: fornisce l'accesso per gestire gli utenti di IAM Identity Center da un provider esterno.

`AWSIdentityCenterExternalManagementPolicy`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIdentityCenterExternalManagementPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 novembre 2025, 00:34 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIdentityCenterExternalManagementPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IdentityStoreUserCreation",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:CreateUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false",
          "identitystore:ReservedUserId" : "false"
        }
      }
    },
    {
      "Sid" : "IdentityStoreUserManagement",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:UpdateUser",
        "identitystore:DeleteUser",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
```

```
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false"
        }
      }
    },
    {
      "Sid" : "IdentityStoreCMKAccess",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : [
            "arn:aws:identitystore::${aws:PrincipalAccount}:identitystore/
${aws:PrincipalTag/IdentityStoreId}"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIdentitySyncFullAccess

Descrizione: concede l'accesso completo al servizio Identity Sync

`AWSIdentitySyncFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIdentitySyncFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 marzo 2022, 23:29 UTC
- Ora modificata: 23 marzo 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication"
      ],
      "Resource" : "arn:*:ds:*:*:*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile",
        "identity-sync:CreateSyncProfile",
        "identity-sync:GetSyncProfile",
        "identity-sync:StartSync",
```

```
        "identity-sync:StopSync",
        "identity-sync:CreateSyncFilter",
        "identity-sync:DeleteSyncFilter",
        "identity-sync:ListSyncFilters",
        "identity-sync:CreateSyncTarget",
        "identity-sync:DeleteSyncTarget",
        "identity-sync:GetSyncTarget",
        "identity-sync:UpdateSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIdentitySyncReadOnlyAccess

Descrizione: accesso in sola lettura al servizio Identity Sync

`AWSIdentitySyncReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIdentitySyncReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 marzo 2022, 23:29 UTC
- Ora modificata: 23 marzo 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSImageBuilderFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni di AWS Image Builder e l'accesso con ambito di risorse ai servizi correlati. AWS

`AWSImageBuilderFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSImageBuilderFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 dicembre 2019, 18:25 UTC
- Ora modificata: 13 aprile 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*imagebuilder*",
        "arn:aws:iam::*:role/*imagebuilder*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3::*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "imagebuilder.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSImageBuilderReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a tutte le azioni di AWS Image Builder.

`AWSImageBuilderReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSImageBuilderReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 dicembre 2019, 22:29 UTC
- Ora modificata: 19 dicembre 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:Get*",
        "imagebuilder:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSImportExportFullAccess

Descrizione: fornisce l'accesso in lettura e scrittura ai lavori creati con Account AWS.

`AWSImportExportFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSImportExportFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSImportExportReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ai lavori creati con Account AWS.

`AWSImportExportReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSImportExportReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:ListJobs",
        "importexport:GetStatus"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIncidentManagerIncidentAccessServiceRolePolicy

Descrizione: concede a Incident Manager le autorizzazioni per chiamare altri AWS servizi come parte della gestione di un incidente.

`AWSIncidentManagerIncidentAccessServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIncidentManagerIncidentAccessServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 novembre 2023, 00:01 UTC
- Ora modificata: 20 febbraio 2024, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIncidentManagerResolverAccess

Descrizione: questa politica concede le autorizzazioni per avviare, visualizzare e aggiornare gli incidenti con accesso completo agli eventi cronologici personalizzati e agli elementi correlati. Assegna questa politica agli utenti che creeranno e risolveranno gli incidenti.

`AWSIncidentManagerResolverAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIncidentManagerResolverAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 maggio 2021, 06:12 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident",
        "ssm-contacts:StartEngagement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentRecordResolverPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:DeleteTimelineEvent",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:UpdateRelatedItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIncidentManagerServiceRolePolicy

Descrizione: questa politica concede a Incident Manager l'autorizzazione a gestire i record degli incidenti e le risorse correlate per conto dell'utente.

`AWSIncidentManagerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 10 maggio 2021, 03:34 UTC
- Ora modificata: 28 gennaio 2025, 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UpdateIncidentRecordPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedOpsItemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentEngagementPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-contacts:StartEngagement",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "PutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IncidentManager",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoT1ClickFullAccess

Descrizione: Fornisce l'accesso completo a AWS IoT 1-Click.

`AWSIoT1ClickFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoT1ClickFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2018, 22:10 UTC
- Ora modificata: 11 maggio 2018, 22:10 UTC

- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoT1ClickReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura a AWS IoT 1-Click.

`AWSIoT1ClickReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoT1ClickReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 maggio 2018, 21:49 UTC
- Ora modificata: 11 maggio 2018, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTAnalyticsFullAccess

Descrizione: Fornisce l'accesso completo a IoT Analytics.

`AWSIoTAnalyticsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTAnalyticsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 giugno 2018, 23:02 UTC
- Ora modificata: 18 giugno 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTAnalyticsReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a IoT Analytics.

`AWSIoTAnalyticsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTAnalyticsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 giugno 2018, 21:37 UTC
- Ora modificata: 18 giugno 2018, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotanalytics:Get*",
        "iotanalytics:SampleChannelData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTConfigAccess

Descrizione: questa policy offre l'accesso completo alle azioni di configurazione AWS IoT

`AWSIoTConfigAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTConfigAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 ottobre 2015, 21:52 UTC

- Ora modificata: 27 settembre 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AcceptCertificateTransfer",
        "iot:AddThingToThingGroup",
        "iot:AssociateTargetsWithJob",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CancelCertificateTransfer",
        "iot:CancelJob",
        "iot:CancelJobExecution",
        "iot:ClearDefaultAuthorizer",
        "iot:CreateAuthorizer",
        "iot:CreateCertificateFromCsr",
        "iot:CreateJob",
        "iot:CreateKeysAndCertificate",
        "iot:CreateOTAUpdate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:CreateRoleAlias",
        "iot:CreateStream",
        "iot:CreateThing",
        "iot:CreateThingGroup",
        "iot:CreateThingType",
        "iot:CreateTopicRule",
```

```
        "iot:DeleteAuthorizer",
        "iot:DeleteCACertificate",
        "iot:DeleteCertificate",
        "iot:DeleteJob",
        "iot:DeleteJobExecution",
        "iot:DeleteOTAUpdate",
        "iot:DeletePolicy",
        "iot:DeletePolicyVersion",
        "iot:DeleteRegistrationCode",
        "iot:DeleteRoleAlias",
        "iot:DeleteStream",
        "iot:DeleteThing",
        "iot:DeleteThingGroup",
        "iot:DeleteThingType",
        "iot:DeleteTopicRule",
        "iot:DeleteV2LoggingLevel",
        "iot:DeprecateThingType",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachPrincipalPolicy",
        "iot:DetachThingPrincipal",
        "iot:DisableTopicRule",
        "iot:EnableTopicRule",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
```

```
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:RegisterCACertificate",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RejectCertificateTransfer",
        "iot:RemoveThingFromThingGroup",
        "iot:ReplaceTopicRule",
        "iot:SearchIndex",
        "iot:SetDefaultAuthorizer",
        "iot:SetDefaultPolicyVersion",
        "iot:SetLoggingOptions",
        "iot:SetV2LoggingLevel",
        "iot:SetV2LoggingOptions",
```

```
        "iot:StartThingRegistrationTask",
        "iot:StopThingRegistrationTask",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
        "iot:TransferCertificate",
        "iot:UpdateAuthorizer",
        "iot:UpdateCACertificate",
        "iot:UpdateCertificate",
        "iot:UpdateEventConfigurations",
        "iot:UpdateIndexingConfiguration",
        "iot:UpdateRoleAlias",
        "iot:UpdateStream",
        "iot:UpdateThing",
        "iot:UpdateThingGroup",
        "iot:UpdateThingGroupsForThing",
        "iot:UpdateAccountAuditConfiguration",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DeleteAccountAuditConfiguration",
        "iot:StartOnDemandAuditTask",
        "iot:CancelAuditTask",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:CreateScheduledAudit",
        "iot:UpdateScheduledAudit",
        "iot:DeleteScheduledAudit",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:CreateSecurityProfile",
        "iot:DescribeSecurityProfile",
        "iot:UpdateSecurityProfile",
        "iot:DeleteSecurityProfile",
        "iot:AttachSecurityProfile",
        "iot:DetachSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTConfigReadOnlyAccess

Descrizione: questa policy consente l'accesso in sola lettura alle azioni di configurazione AWS IoT

`AWSIoTConfigReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTConfigReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 ottobre 2015, 21:52 UTC
- Ora modificata: 27 settembre 2019, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
```

```
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:SearchIndex",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:DescribeSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTDataAccess

Descrizione: questa policy offre l'accesso completo alle azioni di messaggistica AWS IoT

`AWSIoTDataAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTDataAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 ottobre 2015, 21:51 UTC
- Ora modificata: 23 giugno 2021, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:Connect",
        "iot:Publish",
        "iot:Subscribe",
```

```
        "iot:Receive",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow",
        "iot:DeleteThingShadow",
        "iot:ListNamedShadowsForThing"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Descrizione: fornisce accesso in scrittura ai gruppi di oggetti IoT e accesso in lettura ai certificati IoT per l'esecuzione dell'azione di mitigazione ADD_THINGS_TO_THING_GROUP

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:55 UTC
- Ora modificata: 07 agosto 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:ListPrincipalThings",
        "iot:AddThingToThingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTDeviceDefenderAudit

Descrizione: Fornisce accesso in lettura per l'IoT e le risorse correlate

`AWSIoTDeviceDefenderAudit`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTDeviceDefenderAudit` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 18 luglio 2018, 21:17 UTC
- Ora modificata: 25 novembre 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:GetLoggingOptions",
        "iot:GetV2LoggingOptions",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:ListPolicies",
        "iot:GetPolicy",
        "iot:GetEffectivePolicies",
        "iot:ListRoleAliases",
        "iot:DescribeRoleAlias",
        "cognito-identity:GetIdentityPoolRoles",
        "iam:ListRolePolicies",
```

```
        "iam:ListAttachedRolePolicies",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Descrizione: fornisce l'accesso per abilitare la registrazione IoT per l'esecuzione dell'azione di mitigazione ENABLE_IOT_LOGGING

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`è AWS una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:04 UTC
- Ora modificata: 07 agosto 2019, 17:04 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

Descrizione: fornisce ai messaggi l'accesso alla pubblicazione dell'argomento SNS per l'esecuzione dell'azione di mitigazione PUBLISH_FINDING_TO_SNS

`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`è AWS una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:04 UTC
- Ora modificata: 07 agosto 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Descrizione: fornisce l'accesso in scrittura alle policy IoT per l'esecuzione dell'azione di mitigazione REPLACE_DEFAULT_POLICY_VERSION

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:04 UTC
- Ora modificata: 07 agosto 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTDeviceDefenderUpdateCACertMitigationAction

Descrizione: fornisce l'accesso in scrittura ai certificati CA IoT per l'esecuzione dell'azione di mitigazione UPDATE_CA_CERTIFICATE

`AWSIoTDeviceDefenderUpdateCACertMitigationAction`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSIoTDeviceDefenderUpdateCACertMitigationAction` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:05 UTC
- Ora modificata: 07 agosto 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCACertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

Descrizione: fornisce l'accesso in scrittura ai certificati IoT per l'esecuzione dell'azione di mitigazione UPDATE_DEVICE_CERTIFICATE

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 7 agosto 2019, 17:06 UTC
- Ora modificata: 07 agosto 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTDeviceTesterForFreeRTOSFullAccess

Descrizione: consente a AWS IoT Device Tester di eseguire la suite di qualificazione FreerTOS consentendo l'accesso a servizi tra cui IoT, S3 e IAM

`AWSIoTDeviceTesterForFreeRTOSFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSIoTDeviceTesterForFreeRTOSFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 febbraio 2020, 20:33 UTC
- Ora modificata: 10 agosto 2023, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iot:DeleteThing",
        "iot:AttachThingPrincipal",
        "iot:DeleteCertificate",
        "iot:GetRegistrationCode",
        "iot:CreatePolicy",
        "iot:UpdateCACertificate",
        "s3:ListBucket",
        "iot:DescribeEndpoint",
        "iot:CreateOTAUpdate",
        "iot:CreateStream",
        "signer:ListSigningJobs",
        "acm:ListCertificates",
        "iot:CreateKeysAndCertificate",
        "iot:UpdateCertificate",
        "iot:CreateCertificateFromCsr",
        "iot:DetachThingPrincipal",
        "iot:RegisterCACertificate",
        "iot:CreateThing",
        "iam:ListRoles",
        "iot:RegisterCertificate",
        "iot:DeleteCACertificate",
        "signer:PutSigningProfile",
        "s3:ListAllMyBuckets",
        "signer:ListSigningPlatforms",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "signer:StartSigningJob",
        "acm:GetCertificate",
        "signer:DescribeSigningJob",
        "s3:CreateBucket",
        "execute-api:Invoke",
        "s3:DeleteBucket",
        "s3:PutBucketVersioning",
```

```
        "signer:CancelSigningProfile"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:signer:*:*:/signing-profiles/*",
        "arn:aws:signer:*:*:/signing-jobs/*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:acm:*:*:certificate/*",
        "arn:aws:s3:::idt-*",
        "arn:aws:s3:::afr-ota*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream",
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "iot:DeletePolicy",
        "s3:ListBucketVersions",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "iot:DeleteOTAUpdate",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*",
        "arn:aws:iot:*:*:thinggroup/idt*",
        "arn:aws:iam::*:role/idt-*"
      ]
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "s3:DeleteObjectVersion",
        "iot:DeleteOTAUpdate",
        "s3:PutObject",
        "s3:GetObject",
```

```
        "iot:DeleteStream",
        "iot:DeletePolicy",
        "s3:DeleteObject",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "s3:GetObjectVersion",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*",
        "arn:aws:iot:*:*:policy/idt*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:iot:*:*:otaupdate/idt*",
        "arn:aws:iot:*:*:thing/idt*",
        "arn:aws:iot:*:*:cert/*",
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:stream/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : [
        "iot:CancelJobExecution"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:thing/idt*"
      ]
    },
    {
```

```
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
```

```
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ssm:DescribeParameters",
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "Owner"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTDeviceTesterForGreengrassFullAccess

Descrizione: consente a AWS IoT Device Tester di eseguire la suite di qualificazione AWS Greengrass consentendo l'accesso ai servizi correlati tra cui Lambda, IoT, API Gateway, IAM

`AWSIoTDeviceTesterForGreengrassFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSIoTDeviceTesterForGreengrassFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 febbraio 2020, 21:21 UTC
- Ora modificata: 25 giugno 2020, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "lambda.amazonaws.com",
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "iot:DeleteCertificate",
        "lambda:DeleteFunction",
        "execute-api:Invoke",
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:lambda:*:*:function:idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "iot:DeletePolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iot:CreateJob",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:job/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint",
        "greengrass:*",
        "iam:ListAttachedRolePolicies",
        "iot:CreatePolicy",
        "iot:GetThingShadow",
        "iot:CreateKeysAndCertificate",
        "iot:ListThings",
        "iot:UpdateThingShadow",
        "iot:CreateCertificateFromCsr",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "iot:DetachThingPrincipal",
        "iot:AttachThingPrincipal"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
```

```
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketVersions",
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket"
      ],
      "Resource" : "arn:aws:s3:::idt*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTEventsFullAccess

Descrizione: Fornisce accesso completo a IoT Events.

`AWSIoTEventsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTEventsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 gennaio 2019, 22:51 UTC
- Ora modificata: 10 gennaio 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTEventsReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a IoT Events.

`AWSIoTEventsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTEventsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 gennaio 2019, 22:50 UTC
- Ora modificata: 23 settembre 2019, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:Describe*",
        "iotevents:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTFleetHubFederationAccess

Descrizione: Accesso federativo per le applicazioni IoT Fleet Hub

`AWSIoTFleetHubFederationAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTFleetHubFederationAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 15 dicembre 2020, 08:08 UTC
- Ora modificata: 04 aprile 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeIndex",
        "iot:DescribeThingGroup",
        "iot:GetBucketsAggregation",
        "iot:GetCardinality",
        "iot:GetIndexingConfiguration",
        "iot:GetPercentiles",
        "iot:GetStatistics",
```

```
        "iot:SearchIndex",
        "iot:CreateFleetMetric",
        "iot:ListFleetMetrics",
        "iot:DeleteFleetMetric",
        "iot:DescribeFleetMetric",
        "iot:UpdateFleetMetric",
        "iot:DescribeCustomMetric",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListMetricValues",
        "iot:ListThingGroups",
        "iot:ListThingsInThingGroup",
        "iot:ListJobTemplates",
        "iot:DescribeJobTemplate",
        "iot:ListJobs",
        "iot:CreateJob",
        "iot:CancelJob",
        "iot:DescribeJob",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:DescribeJobExecution",
        "iot:ListSecurityProfiles",
        "iot:DescribeSecurityProfile",
        "iot:ListActiveViolations",
        "iot:GetThingShadow",
        "iot:ListNamedShadowsForThing",
        "iot:CancelJobExecution",
        "iot:DescribeEndpoint",
        "iotfleethub:DescribeApplication",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
```

```
      ],
      "Resource" : "arn:aws:sns:*:*:iotfleethub*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:iotfleethub*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTFleetwiseServiceRolePolicy

Descrizione: concede le autorizzazioni alle AWS risorse e ai metadati utilizzati o gestiti da AWSIo TFleetwise per le funzionalità ausiliarie

`AWSIoTFleetwiseServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 settembre 2022, 23:27 UTC

- Ora modificata: 16 ottobre 2025, 04:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTFleetWise",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTFullAccess

Descrizione: questa policy offre l'accesso completo alla configurazione AWS IoT e alle azioni di messaggistica

`AWSIoTFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 ottobre 2015, 15:19 UTC
- Ora modificata: 19 maggio 2022, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:*",
        "iotjobsdata:*"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTLogging

Descrizione: consente la creazione di gruppi Amazon CloudWatch Log e di log di streaming verso i gruppi

`AWSIoTLogging`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTLogging` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 8 ottobre 2015, 15:17 UTC
- Ora modificata: 8 ottobre 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs:DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTManagedIntegrationsFullAccess

Descrizione: Fornisce accesso completo alle integrazioni gestite per AWS IoT Device Management e servizi correlati.

`AWSIoTManagedIntegrationsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTManagedIntegrationsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 marzo 2025, 19:22 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTManagedIntegrationsFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iotmanagedintegrations:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
iotmanagedintegrations.amazonaws.com/AWSServiceRoleForIoTManagedIntegrations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotmanagedintegrations.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTManagedIntegrationsRolePolicy

Descrizione: fornisce integrazioni gestite per l'autorizzazione AWS IoT Device Management a pubblicare log e metriche per tuo conto.

`AWSIoTManagedIntegrationsRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 5 marzo 2025, 21:22 UTC
- Ora modificata: 5 marzo 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTManagedIntegrationsRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTManagedIntegrations",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTOTAUpdate

Descrizione: consente l'accesso per creare AWS IoT Job e descrivere il lavoro di AWS code signer

`AWSIoTOTAUpdate`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTOTAUpdate` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 dicembre 2017, 20:36 UTC
- Ora modificata: 20 dicembre 2017, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateJob",
      "signer:DescribeSigningJob"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIotRoboRunnerFullAccess

Descrizione: questa politica concede autorizzazioni che consentono l'accesso completo all' AWS IoT. RoboRunner

`AWSIotRoboRunnerFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIotRoboRunnerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 29 novembre 2021, 03:54 UTC
- Ora modificata: 23 febbraio 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iotroborunner:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotroborunner.amazonaws.com/
AWSServiceRoleForIoTRoboRunner",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotroborunner.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIotRoboRunnerReadOnly

Descrizione: questa politica concede autorizzazioni che consentono l'accesso in sola lettura all'Iot. AWS RoboRunner

`AWSIotRoboRunnerReadOnly`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSIotRoboRunnerReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 03:43 UTC
- Ora modificata: 16 novembre 2022, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkers",
        "iotroborunner:GetDestination",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIotRoboRunnerServiceRolePolicy

Descrizione: consente RoboRunner all' AWS IoT di gestire AWS le risorse associate per conto del cliente.

`AWSIotRoboRunnerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 febbraio 2023, 16:56 UTC
- Ora modificata: 21 febbraio 2023, 16:56 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/Usage"
        ]
      }
    }
  }
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTRuleActions

Descrizione: consente l'accesso a tutti i AWS servizi supportati in AWS IoT Rule Actions

`AWSIoTRuleActions`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTRuleActions` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 8 ottobre 2015, 15:14 UTC
- Ora modificata: 16 gennaio 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:PutItem",
      "kinesis:PutRecord",
      "iot:Publish",
      "s3:PutObject",
      "sns:Publish",
      "sqs:SendMessage*",
      "cloudwatch:SetAlarmState",
      "cloudwatch:PutMetricData",
      "es:ESHttpPut",
      "firehose:PutRecord"
    ],
```

```
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTSiteWiseConsoleFullAccess

Descrizione: Fornisce l'accesso completo alla gestione dell' AWS IoT SiteWise utilizzando Console di gestione AWS. Nota che questa policy consente anche l'accesso alla creazione e all'elenco degli archivi di dati utilizzati con AWS IoT SiteWise (ad esempio AWS IoT Analytics), l'accesso all'elenco e alla visualizzazione delle risorse AWS IoT Greengrass, l'elenco e la modifica dei segreti di Secrets AWS Manager, il recupero delle thing shadow AWS IoT, l'elenco delle risorse con tag specifici e la creazione e l'utilizzo di un ruolo collegato ai servizi per IoT. AWS SiteWise

`AWSIoTSiteWiseConsoleFullAccess`è una AWS politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTSiteWiseConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 31 maggio 2019, 21:37 UTC
- Ora modificata: 31 maggio 2019, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "iotsitewise:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iotanalytics:List*",
        "iotanalytics:Describe*",
        "iotanalytics:Create*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:GetThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:ListGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
```

```
        "secretsmanager:ListSecrets",
        "secretsmanager:CreateSecret"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:UpdateSecret"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotsitewise.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iotsitewise.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTSiteWiseFullAccess

Descrizione: Fornisce l'accesso completo all'IoT SiteWise.

`AWSIoTSiteWiseFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTSiteWiseFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 dicembre 2018, 20:53 UTC
- Ora modificata: 04 dicembre 2018, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTSiteWiseMonitorPortalAccess

Descrizione: questa policy concede le autorizzazioni per accedere agli SiteWise asset AWS IoT e ai dati degli asset, creare risorse AWS IoT SiteWise Monitor ed elencare gli utenti AWS SSO.

`AWSIoTSiteWiseMonitorPortalAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSIoTSiteWiseMonitorPortalAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 19 maggio 2020, 20:01 UTC

- Ora modificata: 19 maggio 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
```

```
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTSiteWiseMonitorServiceRolePolicy

Descrizione: questo ruolo concede le autorizzazioni di SiteWise monitoraggio AWS IoT per accedere alle risorse e alle proprietà degli SiteWise asset AWS IoT e creare progetti AWS IoT Sitewise, dashboard e politiche di accesso tramite portali IoT. AWS SiteWise

`AWSIoTSiteWiseMonitorServiceRolePolicy`è una policy gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 novembre 2019, 00:59 UTC
- Ora modificata: 13 dicembre 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTSiteWiseReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura all'IoT SiteWise.

`AWSIoTSiteWiseReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTSiteWiseReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 dicembre 2018, 20:55 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:BatchGetAssetPropertyAggregates",
        "iotsitewise:BatchGetAssetPropertyValue",
        "iotsitewise:BatchGetAssetPropertyValueHistory",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAction",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetCompositeModel",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:DescribeAssetModelInterfaceRelationship",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:DescribeBulkImportJob",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeComputationModelExecutionSummary",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeDefaultEncryptionConfiguration",
        "iotsitewise:DescribeExecution",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:DescribeLoggingOptions",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:DescribeStorageConfiguration",
        "iotsitewise:DescribeTimeSeries",
        "iotsitewise:ExecuteQuery",
        "iotsitewise:GetAssetPropertyAggregates",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetInterpolatedAssetPropertyValues",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListActions",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssetRelationships",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
```

```
        "iotsitewise:ListBulkImportJobs",
        "iotsitewise:ListCompositionRelationships",
        "iotsitewise:ListComputationModelDataBindingUsages",
        "iotsitewise:ListComputationModelResolveToResources",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListExecutions",
        "iotsitewise:ListGateways",
        "iotsitewise:ListInterfaceRelationships",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iotsitewise:ListTimeSeries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTThingsRegistration

Descrizione: questa politica consente agli utenti di registrare elementi in blocco utilizzando l'API AWS IoT StartThingRegistrationTask

`AWSIoTThingsRegistration`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTThingsRegistration` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2017, 20:21 UTC
- Ora modificata: 5 ottobre 2020, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AddThingToThingGroup",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateCertificateFromCsr",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:DescribeCertificate",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachThingPrincipal",
        "iot:GetPolicy",
        "iot:ListAttachedPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPrincipalPolicies",
```

```
        "iot:ListPrincipalThings",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RemoveThingFromThingGroup",
        "iot:UpdateCertificate",
        "iot:UpdateThing",
        "iot:UpdateThingGroupsForThing",
        "iot:AddThingToBillingGroup",
        "iot:DescribeBillingGroup",
        "iot:RemoveThingFromBillingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTTwinMakerServiceRolePolicy

Descrizione: consente TwinMaker all' AWS IoT di chiamare altri AWS servizi e di sincronizzare le relative risorse per conto dell'utente.

`AWSIoTTwinMakerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 13 novembre 2023, 18:59 UTC
- Ora modificata: 13 novembre 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SiteWiseAssetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAsset"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAssetModel"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset-model/*"
      ]
```

```
    },
    {
      "Sid" : "SiteWiseAssetModelAndAssetListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TwinMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetEntity",
        "iottwinmaker:CreateEntity",
        "iottwinmaker:UpdateEntity",
        "iottwinmaker:DeleteEntity",
        "iottwinmaker:ListEntities",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:CreateComponentType",
        "iottwinmaker:UpdateComponentType",
        "iottwinmaker:DeleteComponentType",
        "iottwinmaker:ListComponentTypes"
      ],
      "Resource" : [
        "arn:aws:iottwinmaker:*:*:workspace/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTWirelessDataAccess

Descrizione: consente l'accesso ai dati di identità associati ai dispositivi AWS IoT Wireless.

`AWSIoTWirelessDataAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTWirelessDataAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:31 UTC
- Ora modificata: 15 dicembre 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iotwireless:SendDataToWirelessDevice"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTWirelessFullAccess

Descrizione: consente all'identità associata l'accesso completo a tutte le operazioni AWS IoT Wireless.

`AWSIoTWirelessFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTWirelessFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:27 UTC
- Ora modificata: 15 dicembre 2020, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTWirelessFullPublishAccess

Descrizione: fornisce l'accesso completo a IoT Wireless per la pubblicazione su IoT Rules Engine per tuo conto.

`AWSIoTWirelessFullPublishAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTWirelessFullPublishAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:29 UTC
- Ora modificata: 15 dicembre 2020, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTWirelessGatewayCertManager

Descrizione: consente l'accesso all'identità associata per creare, elencare e descrivere i certificati IoT

`AWSIoTWirelessGatewayCertManager`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTWirelessGatewayCertManager` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:30 UTC
- Ora modificata: 15 dicembre 2020, 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTWirelessLogging

Descrizione: consente all'identità associata di creare gruppi Amazon CloudWatch Logs e trasmettere log ai gruppi.

`AWSIoTWirelessLogging`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTWirelessLogging` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 dicembre 2020, 15:32 UTC
- Ora modificata: 15 dicembre 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotwireless*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIoTWirelessReadOnlyAccess

Descrizione: consente all'identità associata di accedere in sola lettura al wireless AWS IoT.

`AWSIoTWirelessReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIoTWirelessReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 15 dicembre 2020, 15:28 UTC
- Ora modificata: 15 dicembre 2020, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:List*",
        "iotwireless:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIPAMServiceRolePolicy

Descrizione: consente a VPC IP Address Manager di accedere alle risorse VPC e di integrarsi con AWS Organizations per tuo conto.

`AWSIPAMServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 30 novembre 2021, 19:08 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListDistributionsByAnycastIpListId",
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    },
    {
      "Sid" : "IPAMAllocationPolicyActions",
      "Effect" : "Allow",
      "Action" : "ec2:AllocateIpamPoolCidr",
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListResolverWriteActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyManagedPrefixList"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:Attribute/ExpectedIpamPrefixListResolverTarget" : "false"
        }
      }
    },
    {
      "Sid" : "PrefixListResolverReadActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIQContractServiceRolePolicy

Descrizione: Utilizzato da AWS IQ per eseguire le richieste di pagamento per conto di un cliente

`AWSIQContractServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 22 agosto 2019, 19:28 UTC
- Ora modificata: 22 agosto 2019, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:Subscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIQFullAccess

Descrizione: Fornisce accesso completo a AWS IQ

`AWSIQFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSIQFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 aprile 2019, 23:13 UTC
- Ora modificata: 25 settembre 2019, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iq:*",
        "iq-permission:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "permission.iq.amazonaws.com",
            "contract.iq.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSIQPermissionServiceRolePolicy

Descrizione: consente a AWS IQ di gestire il ruolo assunto dagli esperti di IQ AWS .

`AWSIQPermissionServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 22 agosto 2019, 19:36 UTC

- Ora modificata: 22 agosto 2019, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

Descrizione: consente l'accesso ai AWS servizi e alle risorse necessari per gli archivi di chiavi personalizzati AWS KMS

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 novembre 2018, 20:10 UTC
- Ora modificata: 10 novembre 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

Descrizione: consente a AWS KMS di sincronizzare le proprietà condivise delle chiavi multiregionali.

`AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 16 giugno 2021, 15:37 UTC
- Ora modificata: 13 novembre 2024, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KMSSynchronizeMultiRegionKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:SynchronizeMultiRegionKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSKeyManagementServicePowerUser

Descrizione: fornisce l'accesso al AWS Key Management Service (KMS).

`AWSKeyManagementServicePowerUser`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSKeyManagementServicePowerUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 07 marzo 2017, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
```

```
        "kms:List*",
        "kms:TagResource",
        "kms:UntagResource",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLakeFormationCrossAccountManager

Descrizione: fornisce l'accesso da più account alle risorse Glue tramite Lake Formation. Garantisce inoltre l'accesso in lettura ad altri servizi richiesti come organizzazioni e gestore dell'accesso alle risorse

`AWSLakeFormationCrossAccountManager`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSLakeFormationCrossAccountManager` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 04 agosto 2020, 20:59 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceSharePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowXAcctManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLakeFormationDataAdmin

Descrizione: Concede l'accesso amministrativo a AWS Lake Formation e ai servizi correlati, come AWS Glue, per la gestione dei data lake

`AWSLakeFormationDataAdmin`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSLakeFormationDataAdmin` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 agosto 2019, 17:33 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLakeFormationDataAdminAllow",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:CreateCatalog",
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTableVersions",
        "glue:GetPartitions",
        "glue:GetTables",
        "glue:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
```

```
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSLakeFormationDataAdminDeny",
      "Effect" : "Deny",
      "Action" : [
        "lakeformation:PutDataLakeSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambda_FullAccess

Descrizione: concede l'accesso completo al servizio AWS Lambda, alle funzionalità della console AWS Lambda e ad altri servizi correlati. AWS

`AWSLambda_FullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSLambda_FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2020, 21:14 UTC

- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "lambda:*",
        "logs:DescribeLogGroups",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
```

```
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lambda.amazonaws.com/
AWSServiceRoleForLambda",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambda_ReadOnlyAccess

Descrizione: concede l'accesso in sola lettura al servizio AWS Lambda, alle funzionalità della console AWS Lambda e ad altri servizi correlati. AWS

`AWSLambda_ReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSLambda_ReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2020, 21:10 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
```

```
        "cloudformation:ListStackResources",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "lambda:Get*",
        "lambda:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:DescribeQueries",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaBasicDurableExecutionRolePolicy

Descrizione: Fornisce autorizzazioni di scrittura per CloudWatch i registri e read/write autorizzazioni per l'esecuzione durevole utilizzate dalle funzioni durevoli APIs Lambda

`AWSLambdaBasicDurableExecutionRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaBasicDurableExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 2 dicembre 2025, 15:04 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicDurableExecutionRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "lambda:CheckpointDurableExecution",
        "lambda:GetDurableExecutionState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaBasicExecutionRole

Descrizione: fornisce autorizzazioni di scrittura per i CloudWatch registri.

`AWSLambdaBasicExecutionRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaBasicExecutionRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 9 aprile 2015, 15:03 UTC
- Ora modificata: 9 aprile 2015, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaDynamoDBExecutionRole

Descrizione: Fornisce accesso in lista e lettura ai flussi DynamoDB e autorizzazioni di scrittura nei log. CloudWatch

`AWSLambdaDynamoDBExecutionRole`[è una politica gestita.AWS]

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaDynamoDBExecutionRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 9 aprile 2015, 15:09 UTC
- Ora modificata: 9 aprile 2015, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
```

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaENIManagementAccess

Descrizione: fornisce le autorizzazioni minime per una funzione Lambda da ENIs gestire (creare, descrivere, eliminare) utilizzata da una funzione Lambda abilitata per VPC.

`AWSLambdaENIManagementAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaENIManagementAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 dicembre 2016, 00:37 UTC
- Ora modificata: 01 ottobre 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaExecute

> **Important**
>
> La policy `AWSLambdaExecute` gestita sta per diventare obsoleta e non è più consigliata per l'uso con AWS Lambda. Utilizza invece `AWSLambdaBasicExecutionRole`. Quando il servizio IAM alla fine renderà obsoleta la policy, non sarà possibile associarla a un ruolo.

Tuttavia, puoi assegnare un ruolo esistente a una risorsa anche se quel ruolo utilizza la politica obsoleta.

Descrizione: fornisce Put, Get Access a S3 e accesso completo ai log. CloudWatch

`AWSLambdaExecute`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaExecute` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaFullAccess

Descrizione: questa politica si trova su un percorso obsoleto. Vedi la documentazione come guida: https://docs.aws.amazon.com/lambda/ latest/dg/access - .html. control-identity-based Fornisce accesso completo a Lambda, S3, DynamoDB, Metrics and Logs. CloudWatch

`AWSLambdaFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 27 novembre 2017, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudwatch:*",
        "cognito-identity:ListIdentityPools",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:SetCognitoEvents",
        "dynamodb:*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "events:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:PassRole",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreateThing",
```

```
        "iot:CreateTopicRule",
        "iot:DescribeEndpoint",
        "iot:GetTopicRule",
        "iot:ListPolicies",
        "iot:ListThings",
        "iot:ListTopicRules",
        "iot:ReplaceTopicRule",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:ListAliases",
        "lambda:*",
        "logs:*",
        "s3:*",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Publish",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sqs:ListQueues",
        "sqs:SendMessage",
        "tag:GetResources",
        "xray:PutTelemetryRecords",
        "xray:PutTraceSegments"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaInvocation-DynamoDB

Descrizione: Fornisce accesso in lettura a DynamoDB Streams.

`AWSLambdaInvocation-DynamoDB`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaInvocation-DynamoDB` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 6 febbraio 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaKinesisExecutionRole

Descrizione: fornisce l'accesso in modalità elenco e lettura agli stream Kinesis e autorizzazioni di scrittura nei log. CloudWatch

`AWSLambdaKinesisExecutionRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaKinesisExecutionRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 9 aprile 2015, 15:14 UTC
- Ora modificata: 19 novembre 2018, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:ListShards",
        "kinesis:ListStreams",
        "kinesis:SubscribeToShard",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaManagedEC2ResourceOperator

Descrizione: questa policy concede le autorizzazioni per creare e amministrare risorse EC2 gestite dalle istanze gestite Lambda e autorizzazioni descrittive.

`AWSLambdaManagedEC2ResourceOperator`AWS è una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaManagedEC2ResourceOperator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2025, 08:34 UTC
- Ora modificata: 10 giugno 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaManagedEC2ResourceOperator`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEncryptionControls"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : "amazon"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*:log-stream:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaMSKExecutionRole

Descrizione: fornisce le autorizzazioni necessarie per accedere al cluster MSK all'interno di un VPC, gestire ENIs (creare, descrivere, eliminare) nel VPC e scrivere le autorizzazioni nei registri. CloudWatch

`AWSLambdaMSKExecutionRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaMSKExecutionRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 agosto 2020, 17:35 UTC

- Ora modificata: 02 agosto 2022, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:GetBootstrapBrokers",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaNetworkConnectorOperatorPolicy

Descrizione: Questa politica concede le autorizzazioni per creare e amministrare le risorse ENI gestite dal Lambda Network Connector

`AWSLambdaNetworkConnectorOperatorPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaNetworkConnectorOperatorPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 giugno 2026, 15:27 UTC
- Ora modificata: 22 giugno 2026, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaNetworkConnectorOperatorPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateEniInAnySubnet",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Sid" : "AllowCreateEniWithSecurityGroups",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "AllowCreateEniWithLambdaTagKeys",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:lambda:networkConnectorName",
            "aws:lambda:networkConnectorId"
          ]
        }
      }
    },
    {
      "Sid" : "TagENIOnCreate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "ec2:ManagedResourceOperator" : "network-connectors.lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaReplicator

Descrizione: concede a Lambda Replicator le autorizzazioni necessarie per replicare le funzioni tra le regioni

`AWSLambdaReplicator`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 23 maggio 2017, 17:53 UTC
- Ora modificata: 08 dicembre 2017, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "LambdaCreateDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DisableReplication"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "IamPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFrontListDistributions",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionsByLambdaFunction"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaRole

Descrizione: politica predefinita per il ruolo del servizio AWS Lambda.

`AWSLambdaRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaServiceRolePolicy

Descrizione: consente a Lambda di descrivere e terminare le istanze gestite da EC2 per tuo conto.

`AWSLambdaServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 30 novembre 2025, 08:04 UTC
- Ora modificata: 22 giugno 2026, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "network-connectors.lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaSQSQueueExecutionRole

Descrizione: fornisce l'accesso agli attributi di ricezione, eliminazione di messaggi e lettura alle code SQS e autorizzazioni di scrittura per i log. CloudWatch

`AWSLambdaSQSQueueExecutionRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaSQSQueueExecutionRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 giugno 2018, 21:50 UTC
- Ora modificata: 14 giugno 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLambdaVPCAccessExecutionRole

Descrizione: fornisce autorizzazioni minime per l'esecuzione di una funzione Lambda durante l'accesso a una risorsa all'interno di un VPC: creazione, descrizione, eliminazione di interfacce di rete e autorizzazioni di scrittura nei registri. CloudWatch

`AWSLambdaVPCAccessExecutionRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSLambdaVPCAccessExecutionRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 febbraio 2016, 23:15 UTC
- Ora modificata: 5 gennaio 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLambdaVPCAccessExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLicenseManagerConsumptionPolicy

Descrizione: fornisce le autorizzazioni per consentire l'accesso alle azioni dell'API AWS License Manager necessarie per utilizzare le licenze per le quali l'utente dispone dei diritti.

`AWSLicenseManagerConsumptionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSLicenseManagerConsumptionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 agosto 2021, 23:18 UTC
- Ora modificata: 11 agosto 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Descrizione: consente al servizio AWS License Manager Linux Subscriptions di gestire le risorse per conto dell'utente.

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 dicembre 2022, 18:54 UTC
- Ora modificata: 08 luglio 2024, 22:04 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLicenseManagerMasterAccountRolePolicy

Descrizione: politica del ruolo dell'account principale del servizio AWS License Manager

`AWSLicenseManagerMasterAccountRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 novembre 2018, 19:03 UTC
- Ora modificata: 31 maggio 2022, 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*/resource_sync/*"
      ]
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
```

```
        "athena:StartQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations",
        "ram:TagResource"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Service" : "LicenseManager"
        }
      }
    },
    {
      "Sid" : "RAMPermissions3",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "LicenseManager"
        }
      }
    },
    {
      "Sid" : "IAMGetRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "IAMPassRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudformationPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/
LicenseManagerCrossAccountCloudDiscoveryStack/*"
      ]
    },
    {
      "Sid" : "GlueUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:UpdateJob",
        "glue:UpdateCrawler"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:crawler/LicenseManagerResourceSynDataCrawler",
        "arn:aws:glue:*:*:job/LicenseManagerResourceSynDataProcessJob",
        "arn:aws:glue:*:*:table/license_manager_resource_inventory_db/*",
        "arn:aws:glue:*:*:table/license_manager_resource_sync/*",
        "arn:aws:glue:*:*:database/license_manager_resource_inventory_db",
        "arn:aws:glue:*:*:database/license_manager_resource_sync"
      ]
    },
    {
      "Sid" : "RGPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:PutGroupPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLicenseManagerMemberAccountRolePolicy

Descrizione: politica relativa al ruolo degli account dei membri del servizio AWS License Manager

`AWSLicenseManagerMemberAccountRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 novembre 2018, 19:04 UTC
- Ora modificata: 15 novembre 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:GetLicenseConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync",
        "ssm:ListResourceDataSync",
        "ssm:ListAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLicenseManagerServiceRolePolicy

Descrizione: politica dei ruoli predefiniti del servizio AWS License Manager

`AWSLicenseManagerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 novembre 2018, 19:02 UTC
- Ora modificata: 19 novembre 2025, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "IAMPermissionsForCreatingMemberSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3BucketPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSTopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeHosts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
```

```
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*::document/AWSLicenseManager-*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:GetServiceSettings",
        "license-manager:GetLicense*",
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Descrizione: consente al servizio AWS License Manager User Subscriptions di gestire le risorse per conto dell'utente.

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 30 luglio 2022, 01:17 UTC
- Ora modificata: 10 luglio 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:GetAuthorizedApplicationDetails",
        "ds:DescribeTrusts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2WritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:productCode" : [
            "bz0vcy31ooqlzk5tsash4r1ik",
            "d44g89hc0gp9jdzm99rznthpw",
```

```
            "77yzkpa7kvee1y1tt7wnsdwoc",
            "a8jthu9h8pjsn4b8ylvfl6sfr",
            "7at6der8hnlov1g347e6tdkde",
            "3t0v0vuhvxjzm6m462f9v8iz4",
            "4gs2prcp03ojilgkjx8m3ifh7",
            "5uypd9kpy863kwykrwn4bcolv",
            "eqtok9gt75we12qgk28b955qc"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SSMDocumentExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunPowerShellScript"
      ]
    },
    {
      "Sid" : "SSMInstanceExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSLicenseManager" : "UserSubscriptions"
        }
      }
    },
    {
      "Sid" : "ReadHostedZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
```

```
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecurityGroupRulePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Sid" : "DescribeSubnetsPermissions",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecretPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:license-manager-user-*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSM2ServicePolicy

Descrizione: consente a AWS M2 di gestire AWS le risorse per tuo conto.

`AWSM2ServicePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 07 giugno 2022, 20:26 UTC
- Ora modificata: 07 giugno 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
```

```
            "AWS/M2"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedAccountManagementAccess

Descrizione: concede AWS le autorizzazioni per aggiornare e mantenere i ruoli AWS gestiti per gli AWS account gestiti

`AWSManagedAccountManagementAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSManagedAccountManagementAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 luglio 2026, 19:57 UTC
- Ora modificata: 20 luglio 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAccountManagementAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachRolePolicy",
      "iam:CreateRole",
      "iam:DeleteRole",
      "iam:DeleteRolePermissionsBoundary",
      "iam:DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:PutRolePermissionsBoundary",
      "iam:PutRolePolicy",
      "iam:TagRole",
      "iam:UntagRole",
      "iam:UpdateAssumeRolePolicy",
      "iam:UpdateRole"
    ],
    "Resource" : "arn:*:iam::*:role/managed/*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedAccountUserEntitlementAccess

Descrizione: concede AWS le autorizzazioni per gestire i diritti di accesso all'account per gli account gestiti AWS

`AWSManagedAccountUserEntitlementAccess`è una politica gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AWSManagedAccountUserEntitlementAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 luglio 2026, 21:42 UTC
- Ora modificata: 17 luglio 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAccountUserEntitlementAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "identitystore:CreateGroup",
      "identitystore:GetGroupId",
      "identitystore:GetUserId",
      "identitystore:CreateGroupMembership",
      "sso:ListInstances",
      "sso-directory:ListProvisioningTenants",
      "account-access:ListApplications",
      "account-access:CreateEntitlement",
      "account-access:ListEntitlements"
    ],
    "Resource" : "*"
  }
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedAdvancedFeaturesActivationAccess

Descrizione: concede AWS l'autorizzazione ad attivare funzionalità avanzate per gli account AWS gestiti

`AWSManagedAdvancedFeaturesActivationAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSManagedAdvancedFeaturesActivationAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 luglio 2026, 14:27 UTC
- Ora modificata: 21 luglio 2026, 14:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAdvancedFeaturesActivationAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "iam:PutAccountProperties"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedBudgetsSpendLimitManagementAccess

Descrizione: concede al servizio AWS Budgets le autorizzazioni per allegare e scollegare le politiche di controllo del servizio e gestire gli account in un' AWS organizzazione per far rispettare i limiti di spesa sugli account dei membri.

`AWSManagedBudgetsSpendLimitManagementAccess`è una politica gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AWSManagedBudgetsSpendLimitManagementAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 luglio 2026, 21:12 UTC
- Ora modificata: 17 luglio 2026, 21:12 UTC

- ARN: `arn:aws:iam::aws:policy/AWSManagedBudgetsSpendLimitManagementAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SCPActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:DescribePolicy",
        "organizations:DetachPolicy",
        "organizations:ListPolicies"
      ],
      "Resource" : "arn:aws:organizations::*:policy/*/service_control_policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedBy" : "SpendLimit"
        }
      }
    },
    {
      "Sid" : "SCPTargetActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Sid" : "AccountActions",
```

```
      "Effect" : "Allow",
      "Action" : "organizations:CloseAccount",
      "Resource" : "arn:aws:organizations::*:account/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedControlPolicyManagementAccess

Descrizione: concede AWS l'autorizzazione a gestire le politiche di controllo dell'organizzazione per gli account AWS gestiti

`AWSManagedControlPolicyManagementAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSManagedControlPolicyManagementAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 luglio 2026, 14:27 UTC
- Ora modificata: 21 luglio 2026, 14:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedControlPolicyManagementAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribePolicy",
      "organizations:UpdatePolicy",
      "organizations:ListPolicies",
      "organizations:ListRoots",
      "organizations:CreatePolicy",
      "organizations:AttachPolicy",
      "organizations:DetachPolicy",
      "organizations:DeletePolicy",
      "organizations:TagResource",
      "organizations:UntagResource",
      "organizations:ListTagsForResource"
    ],
    "Resource" : "*"
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedServiceAccessManagementAccess

Descrizione: concede le autorizzazioni per gestire le politiche di controllo dei servizi (SCP) nelle AWS organizzazioni per il servizio AWS Managed Service Access Management. Include le autorizzazioni

per elencare, creare, aggiornare e allegare SCP con ambito alle politiche contrassegnate con =service-access. ManagedBy

`AWSManagedServiceAccessManagementAccess`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AWSManagedServiceAccessManagementAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica relativa al ruolo del servizio
- Ora di creazione: 21 luglio 2026, 17:57 UTC
- Ora modificata: 21 luglio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSManagedServiceAccessManagementAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowListRoots",
      "Effect" : "Allow",
      "Action" : "organizations:ListRoots",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSCPList",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY"
        }
      }
    },
    {
      "Sid" : "AllowSCPCreateWithTag",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CreatePolicy",
        "organizations:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY",
          "aws:RequestTag/ManagedBy" : "service-access"
        }
      }
    },
    {
      "Sid" : "AllowSCPUpdateTagged",
      "Effect" : "Allow",
      "Action" : "organizations:UpdatePolicy",
      "Resource" : "arn:aws:organizations::*:policy/*/service_control_policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedBy" : "service-access"
        }
      }
    },
    {
      "Sid" : "AllowSCPAttachTaggedPolicy",
      "Effect" : "Allow",
      "Action" : "organizations:AttachPolicy",
      "Resource" : "arn:aws:organizations::*:policy/*/service_control_policy/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/ManagedBy" : "service-access"
        }
      }
    },
    {
      "Sid" : "AllowSCPAttachRoot",
      "Effect" : "Allow",
      "Action" : "organizations:AttachPolicy",
      "Resource" : "arn:aws:organizations::*:root/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedServices_ContactsServiceRolePolicy

Descrizione: consente AWS a Managed Services di leggere i valori dei tag sulle AWS risorse

`AWSManagedServices_ContactsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 23 marzo 2023, 17:07 UTC
- Ora modificata: 23 marzo 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "tag:GetResources",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetBucketTagging",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:authType" : "REST-HEADER",
          "s3:signatureversion" : "AWS4-HMAC-SHA256"
        },
        "NumericGreaterThanEquals" : {
          "s3:TlsVersion" : "1.2"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

Descrizione: AWS Managed Services: policy per gestire l'infrastruttura dei controlli investigativi

`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 dicembre 2022, 23:11 UTC
- Ora modificata: 19 dicembre 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateTermination*",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-recorder",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-rules-cdk",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-infrastructure-cdk"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeAggregationAuthorizations",
        "config:PutAggregationAuthorization",
        "config:TagResource",
        "config:PutConfigRule"
      ],
      "Resource" : [
        "arn:aws:config:*:*:aggregation-authorization/540708452589/*",
        "arn:aws:config:*:*::config-rule/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutObject",
```

```
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-config-record-bucket-*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedServices_EventsServiceRolePolicy

Descrizione: policy di AWS Managed Services per abilitare la funzionalità del processore di eventi AMS.

`AWSManagedServices_EventsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 07 febbraio 2023, 18:41 UTC
- Ora modificata: 07 febbraio 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "events.managedservices.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedServices_SelfServiceReporting_ServiceRolePolicy

Descrizione: consente alla funzionalità Self Service Reporting di Amazon AWS Managed Service di leggere i dati AWS dell'organizzazione per tuo conto per abilitare il reporting aggregato a livello di organizzazione

`AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 8 gennaio 2025, 21:22 UTC
- Ora modificata: 08 gennaio 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedServicesDeploymentToolkitPolicy

Descrizione: consente AWS a Managed Services di gestire il toolkit di distribuzione per conto dell'utente.

`AWSManagedServicesDeploymentToolkitPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 09 giugno 2022, 18:33 UTC
- Ora modificata: 04 aprile 2024, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AMSCDKToolkitS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:ListBucket",
        "s3:ListBucketVersions",
```

```
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
    },
    {
      "Sid" : "AMSCDKToolkitCloudFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:GetTemplateSummary",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
    },
    {
      "Sid" : "AMSCDKToolkitECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:CreateRepository",
        "ecr:DeleteLifecyclePolicy",
        "ecr:DeleteRepository",
        "ecr:DeleteRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:ListTagsForResource",
```

```
        "ecr:PutImageScanningConfiguration",
        "ecr:PutImageTagMutability",
        "ecr:PutLifecyclePolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedSettingsAdminAccess

Descrizione: concede l'accesso amministrativo completo alla gestione Account AWS delle impostazioni. Questa politica consente ai proprietari di visualizzare e modificare le informazioni sull'account, la fatturazione, i pagamenti, la registrazione fiscale, la gestione delle identità, le politiche organizzative, i budget, l'analisi dei costi e le notifiche dell'area di lavoro. Destinato ai proprietari di aree di lavoro che necessitano di un accesso amministrativo completo alla configurazione degli account e alla gestione dei membri. La policy non consente l'accesso a servizi di elaborazione, archiviazione, rete o altri servizi di infrastruttura non correlati alle impostazioni dell'account.

`AWSManagedSettingsAdminAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSManagedSettingsAdminAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 luglio 2026, 01:27 UTC
- Ora modificata: 23 luglio 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedSettingsAdminAccess`

Versione della politica

Versione della politica: v2 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ActivateAdvancedUpdateAccountName",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAccountName"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSettingsAccountAccess",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "account:CloseAccount",
        "account:PutAccountName",
        "account:PutContactInformation",
        "account:StartPrimaryEmailUpdate",
        "account:AcceptPrimaryEmailUpdate",
        "account:GetPrimaryEmailUpdateStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsBillingAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "billing:GetCredits",
        "billing:GetSellerOfRecord",
        "billing:RedeemCredits"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsCostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage",
        "ce:GetCostForecast"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsBudgetsAccess",
      "Effect" : "Allow",
      "Action" : [
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ModifyBudget",
        "budgets:ViewBudget",
        "budgets:UpdateBudget",
        "budgets:CreateBudget",
        "budgets:DeleteBudget",
        "budgets:DescribeBudgets",
        "budgets:DescribeBudget",
        "budgets:DescribeBudgetActionHistories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsIAMPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/managed/
AWSManagedBudgetsSpendLimitManagementRole",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSettingsCustomerVerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "customer-verification:UpdateCustomerVerificationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsFreeTierAccess",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState",
        "freetier:UpgradeAccountPlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsIdentityStoreAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:CreateGroup",
        "identitystore:CreateGroupMembership",
        "identitystore:CreateUser",
        "identitystore:DeleteGroup",
        "identitystore:DeleteGroupMembership",
        "identitystore:DeleteUser",
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetUserId",
        "identitystore:ListGroupMemberships",
        "identitystore:UpdateIdentityStore",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
```

```
        "identitystore:ReserveUser",
        "identitystore:UpdateGroup",
        "identitystore:UpdateUser",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "builderid:CreateInvitation",
        "builderid:DeleteInvitation",
        "builderid:DisassociateCollaborator",
        "builderid:ListInvitations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsInvoicingAccess",
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CloseAccount",
        "organizations:CreatePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:CreateBuilderIdOwnedAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeAccount",
        "organizations:InviteAccountToOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsOrganizationsAiOptOutPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "AISERVICES_OPT_OUT_POLICY"
        }
      }
    },
    {
      "Sid" : "AWSSettingsPaymentsAccess",
      "Effect" : "Allow",
      "Action" : [
        "payments:CreatePaymentInstrument",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:MakePayment",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:ListTagsForResource",
        "payments:BatchGetPaymentProfiles",
        "payments:AcceptTermsAndConditionsForProgramByAccountId",
        "payments:CreatePaymentAttempt",
        "payments:CreatePaymentProfile",
        "payments:Get",
        "payments:GetAcceptedTermsAndConditionsForProgramByAccountId",
        "payments:GetEligibleCurrencies",
        "payments:GetPaymentAttempt",
        "payments:GetPaymentPreferences",
        "payments:GetPreferredCurrency",
        "payments:GetRecommendedTermsAndConditionsForProgram",
        "payments:ListPaymentProfiles",
        "payments:SearchFinancialRecords",
        "payments:SetPreferredCurrency",
        "payments:UpdatePaymentProfile",
        "payments:GetAccountBalance"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AWSSettingsSESAccess",
      "Effect" : "Allow",
      "Action" : [
        "ses:SendEmail"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsSSOAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DeleteApplicationAssignment",
        "sso:DescribeInstance",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:ListApplicationAssignments",
        "sso:CreateApplicationAssignment",
        "sso:DescribeApplication",
        "sso:ListApplications",
        "sso:UpdateInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsTaxAccess",
      "Effect" : "Allow",
      "Action" : [
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsSupportAccess",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
```

```
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ActivateAdvancedProvisioningAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CreateBuilderIdOwnedAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:ListAccounts",
        "sso:ListInstances",
        "identitystore:GetUserId",
        "sso-directory:ListProvisioningTenants",
        "account-access:ListApplications",
        "account-access:CreateApplication",
        "account-access:CreateEntitlement",
        "signin:DeleteConsoleAuthorizationConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedDelegatedAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com",
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "ActivateAdvancedManagedRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:ListAttachedRolePolicies",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/managed/*",
        "arn:aws:iam::*:role/ManagedAccountAdmin",
        "arn:aws:iam::*:role/AccountFullAccessRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedMemberAccountAssume",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/managed/
AWSManagedAdvancedFeaturesActivationRole",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedBudgetsAccess",
      "Effect" : "Allow",
      "Action" : "budgets:ModifyBudget",
      "Resource" : "arn:aws:budgets::*:budget/sla-*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "ActivateAdvancedSCPCleanupAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DeletePolicy",
        "organizations:DetachPolicy",
        "organizations:ListPolicies",
        "organizations:ListRoots"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedSettingsReadOnlyAccess

Descrizione: concede ai membri del team l'accesso in sola lettura alle AWS Impostazioni, incluse le informazioni sull'area di lavoro e sul proprietario, l'appartenenza al team, il piano e il riepilogo della spesa. Non concede le autorizzazioni per modificare la configurazione dell'area di lavoro o per gestire la fatturazione e i pagamenti.

`AWSManagedSettingsReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSManagedSettingsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 luglio 2026, 01:12 UTC
- Ora modificata: 23 luglio 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedSettingsReadOnlyAccess`

Versione della politica

Versione della politica: v2 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IdentityStoreReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "OrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagedSignUpAdminAccess

Descrizione: concede AWS l'autorizzazione a completare la registrazione per gli account AWS gestiti.

`AWSManagedSignUpAdminAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSManagedSignUpAdminAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica relativa al ruolo del servizio
- Ora di creazione: 20 luglio 2026, 19:27 UTC
- Ora modificata: 20 luglio 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSManagedSignUpAdminAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PaymentWidgetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "payments:CreatePaymentInstrument",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:ListTagsForResource",
        "payments:MakePayment",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BillingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "billing:GetSellerOfRecord"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "account:GetContactInformation"
      ],
      "Resource" : "arn:aws:account::*:account"
    },
    {
      "Sid" : "InvoicingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TaxWidgetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerVerificationWidgetPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "customer-verification:UpdateCustomerVerificationDetails"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagementConsoleAdministratorAccess

Descrizione: fornisce l'accesso completo per configurare e personalizzare il Console di gestione AWS

`AWSManagementConsoleAdministratorAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSManagementConsoleAdministratorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: Job function policy
- Ora di creazione: 14 agosto 2025, 21:19 UTC
- Ora modificata: 23 marzo 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AWSManagementConsoleAdministratorAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "uxc:PutAccountColor",
        "uxc:DeleteAccountColor",
        "uxc:GetAccountCustomizations",
        "uxc:UpdateAccountCustomizations",
        "uxc:ListServices",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:AssociateChannel",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:AssociateManagedNotificationAdditionalChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DeregisterNotificationHub",
        "notifications:DisableNotificationsAccessForOrganization",
        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
```

```
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListManagedNotificationChildEvents",
        "notifications:ListManagedNotificationConfigurations",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:DeleteEnvironment",
        "cloudshell:GetFileDownloadUrls",
        "cloudshell:GetFileUploadUrls",
        "cloudshell:DescribeEnvironments",
        "cloudshell:PutCredentials",
        "cloudshell:StartEnvironment",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetView",
```

```
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSManagementConsoleBasicUserAccess

Descrizione: concede l'accesso alle Console di gestione AWS funzionalità essenziali e alle funzionalità di esperienza utente (UX) per utenti non amministrativi.

`AWSManagementConsoleBasicUserAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSManagementConsoleBasicUserAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 14 agosto 2025, 20:34 UTC
- Ora modificata: 17 marzo 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagementConsoleBasicUserAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "uxc:GetAccountCustomizations",
        "uxc:ListServices",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationEvent",
        "notifications:ListManagedNotificationChildEvents",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:StartEnvironment",
        "cloudshell:DeleteEnvironment",
        "cloudshell:PutCredentials",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
```

```
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceAmiIngestion

Descrizione: Consente di AWS Marketplace copiare le tue Amazon Machine Images (AMIs) per elencarle su AWS Marketplace

`AWSMarketplaceAmiIngestion`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceAmiIngestion` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 settembre 2020, 20:55 UTC
- Ora modificata: 25 settembre 2020, 20:55 UTC

- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:ec2:us-east-1::snapshot/snap-*"
    },
    {
      "Action" : [
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceDeploymentServiceRolePolicy

Descrizione: consente di AWS Marketplace creare e gestire i parametri di distribuzione del venditore per i prodotti a cui ti abboni AWS Marketplace.

`AWSMarketplaceDeploymentServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 novembre 2023, 23:34 UTC
- Ora modificata: 15 novembre 2023, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RemoveRegionsFromReplication"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TagMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/expirationDate" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "expirationDate"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceDiscoveryFullAccess

Descrizione: fornisce l'accesso completo all'API AWS Marketplace Discovery per la ricerca e il recupero di informazioni sui prodotti e sui prezzi.

`AWSMarketplaceDiscoveryFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceDiscoveryFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 maggio 2026, 17:12 UTC
- Ora modificata: 07 maggio 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceDiscoveryFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetListing",
        "aws-marketplace:GetProduct",
        "aws-marketplace:GetOffer",
        "aws-marketplace:GetOfferTerms",
        "aws-marketplace:GetOfferSet",
        "aws-marketplace:ListPurchaseOptions",
        "aws-marketplace:ListFulfillmentOptions",
        "aws-marketplace:SearchListings",
        "aws-marketplace:SearchFacets"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/product/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/listing/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offer/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offerSet/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/purchaseOption/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceFullAccess

Descrizione: offre la possibilità di sottoscrivere e annullare l'iscrizione al AWS Marketplace software, consente agli utenti di gestire le istanze del software Marketplace dalla pagina «Il tuo software» di Marketplace e fornisce l'accesso amministrativo a EC2.

`AWSMarketplaceFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 febbraio 2015, 17:21 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:DescribeInstanceStatus",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:CreateTopic",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceGetEntitlements

Descrizione: fornisce l'accesso in lettura ai AWS Marketplace diritti

`AWSMarketplaceGetEntitlements`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceGetEntitlements` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 27 marzo 2017, 19:37 UTC
- Ora modificata: 5 aprile 2024, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceImageBuildFullAccess

Descrizione: fornisce l'accesso completo alla funzione AWS Marketplace Private Image Build. Oltre a creare immagini private, fornisce anche le autorizzazioni per aggiungere tag alle immagini, avviare e terminare le istanze ec2.

`AWSMarketplaceImageBuildFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceImageBuildFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 31 luglio 2018, 23:29 UTC
- Ora modificata: 04 marzo 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:StartBuild",
        "aws-marketplace:DescribeBuilds"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/marketplace-image-build:build-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*Automation*",
        "arn:aws:iam::*:role/*Instance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "ec2:DeregisterImage",
        "ec2:CopyImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:RunInstances",
        "ec2:DescribeInstanceStatus",
        "sns:GetTopicAttributes",
        "iam:GetRole",
```

```
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
```

```
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
            "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
            "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
            "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
            "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
            "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
            "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
            "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/marketplace-image-build:build-id" : "*"
        },
        "StringNotEquals" : {
```

```
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceLicenseManagementServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da AWS Marketplace per la gestione delle licenze.

`AWSMarketplaceLicenseManagementServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 03 dicembre 2020, 08:33 UTC
- Ora modificata: 03 dicembre 2020, 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListReceivedGrants",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant",
        "license-manager:AcceptGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceManageSubscriptions

Descrizione: offre la possibilità di sottoscrivere e annullare l'iscrizione al software AWS Marketplace

`AWSMarketplaceManageSubscriptions`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceManageSubscriptions` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 07 maggio 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetListing",
        "aws-marketplace:GetProduct",
        "aws-marketplace:GetOffer",
        "aws-marketplace:GetOfferTerms",
        "aws-marketplace:GetOfferSet",
        "aws-marketplace:ListPurchaseOptions",
        "aws-marketplace:ListFulfillmentOptions",
        "aws-marketplace:SearchFacets",
        "aws-marketplace:SearchListings"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/product/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/listing/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offer/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offerSet/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/purchaseOption/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:UpdatePurchaseOrders",
        "aws-marketplace:ListAgreementCharges",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:AcceptAgreementPaymentRequest",
        "aws-marketplace:RejectAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
```

```
            "PurchaseAgreement"
          ]
        },
        "Null" : {
          "aws-marketplace:AgreementType" : "false"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
    },
    {
      "Sid" : "AWSMarketplaceTokenManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AgentTokenContainer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateAgentTokenContainer",
            "RequestExpressPrivateOffer",
            "ExpireToken"
          ]
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceEntityReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceAgreementCancellationRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest",
        "aws-marketplace:AcceptAgreementCancellationRequest",
        "aws-marketplace:CancelAgreement",
        "aws-marketplace:RejectAgreementCancellationRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Acceptor"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceMeteringFullAccess

Descrizione: fornisce l'accesso completo a AWS Marketplace Metering.

`AWSMarketplaceMeteringFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceMeteringFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 marzo 2016, 22:39 UTC
- Ora modificata: 17 marzo 2016, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:MeterUsage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceMeteringRegisterUsage

Descrizione: fornisce le autorizzazioni per registrare una risorsa e tenere traccia dell'utilizzo tramite il servizio di AWS Marketplace misurazione.

`AWSMarketplaceMeteringRegisterUsage`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceMeteringRegisterUsage` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 novembre 2019, 01:17 UTC
- Ora modificata: 21 novembre 2019, 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:RegisterUsage"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceProcurementSystemAdminFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni amministrative per un'integrazione di AWS Marketplace eProcurement.

`AWSMarketplaceProcurementSystemAdminFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceProcurementSystemAdminFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 giugno 2019, 13:07 UTC
- Ora modificata: 21 aprile 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*",
        "invoicing:CreateProcurementPortalPreference",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:ListProcurementPortalPreferences"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplacePurchaseOrdersServiceRolePolicy

Descrizione: consente l'accesso ai AWS Marketplace servizi per la gestione degli ordini di acquisto.

`AWSMarketplacePurchaseOrdersServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 27 ottobre 2021, 15:12 UTC
- Ora modificata: 27 ottobre 2021, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceRead-only

Descrizione: offre la possibilità di rivedere AWS Marketplace gli abbonamenti

`AWSMarketplaceRead-only`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceRead-only` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 07 maggio 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:ListAgreementCharges",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListInstanceProfiles",
        "sns:GetTopicAttributes",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetListing",
```

```
        "aws-marketplace:GetProduct",
        "aws-marketplace:GetOffer",
        "aws-marketplace:GetOfferTerms",
        "aws-marketplace:GetOfferSet",
        "aws-marketplace:ListPurchaseOptions",
        "aws-marketplace:ListFulfillmentOptions",
        "aws-marketplace:SearchFacets",
        "aws-marketplace:SearchListings"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/product/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/listing/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offer/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offerSet/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/purchaseOption/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceResaleAuthorizationServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da AWS Marketplace For Resale Authorization.

`AWSMarketplaceResaleAuthorizationServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 5 marzo 2024, 18:47 UTC
- Ora modificata: 01 agosto 2025, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "aws-marketplace:Entity"
```

```
        },
        "ArnLike" : {
          "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
        },
        "Null" : {
          "ram:Principal" : "true"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "Null" : {
          "ram:Principal" : "false"
        },
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAcceptDelete",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:DeleteResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
```

```
      "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ]
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceSellerFullAccess

Descrizione: fornisce l'accesso completo a tutte le operazioni del venditore su AWS Marketplace e ad altri AWS servizi come la gestione delle AMI.

`AWSMarketplaceSellerFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceSellerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 luglio 2019, 20:40 UTC
- Ora modificata: 21 luglio 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Versione della politica

Versione della politica: v32 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:uploadFiles",
        "aws-marketplace-management:viewReports",
        "aws-marketplace-management:viewSupport",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
```

```
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:GetSellerDashboard",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AgreementAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AssetScanning",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsights",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*",
        "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/*",
        "arn:aws:aws-marketplace:*:*:verification-type/*/verification-evidence/*",
        "arn:aws:aws-marketplace:*:*:tax-compliance-profile/*",
        "arn:aws:aws-marketplace:*:*:tax-compliance-profile-change-task/*"
      ]
    },
    {
      "Sid" : "SellerSettings",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace-management:GetSellerVerificationDetails",
        "aws-marketplace-management:PutSellerVerificationDetails",
        "aws-marketplace-management:GetBankAccountVerificationDetails",
        "aws-marketplace-management:PutBankAccountVerificationDetails",
        "aws-marketplace-management:GetSecondaryUserVerificationDetails",
        "aws-marketplace-management:PutSecondaryUserVerificationDetails",
        "aws-marketplace-management:GetAdditionalSellerNotificationRecipients",
        "aws-marketplace-management:PutAdditionalSellerNotificationRecipients",
        "payments:GetPaymentInstrument",
        "payments:CreatePaymentInstrument",
        "tax:GetTaxInterview",
        "tax:PutTaxInterview",
        "tax:GetTaxInfoReportingDocument",
        "tax:ListSupplementalTaxRegistrations",
        "tax:PutSupplementalTaxRegistration",
        "tax:DeleteSupplementalTaxRegistration",
        "tax:GetTaxRegistration",
        "tax:PutTaxRegistration",
        "tax:ListTaxRegistrations",
        "aws-marketplace:ListPayables",
        "aws-marketplace:ListInvoiceSubmissionTasks",
        "invoicing:ListInvoiceSummaries",
        "invoicing:GetInvoicePDF",
        "aws-marketplace:ListIssuedTaxInvoices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceSellerVerificationEvidenceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateVerificationEvidence",
        "aws-marketplace:UpdateVerificationEvidence",
        "aws-marketplace:GetVerificationEvidence"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:verification-type/*/verification-
evidence/*"
    },
    {
      "Sid" : "MarketplaceSellerVerificationManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListVerificationEvidence",
        "aws-marketplace:StartVerification",
```

```
        "aws-marketplace:GetVerification",
        "aws-marketplace:ListVerifications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvoiceSubmissionManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartInvoiceSubmissionTask",
        "aws-marketplace:GetInvoiceSubmissionTask"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/invoice-
submission-task/*"
    },
    {
      "Sid" : "MarketplaceEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-files/
${aws:PrincipalAccount}/*"
      ]
    },
    {
      "Sid" : "Support",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourcePolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*",
```

```
        "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "resale-authorization.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgreementPaymentRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SendAgreementPaymentRequest",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:CancelAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartVerification",
        "partnercentral:GetVerification"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SellerSettingsGetIssuedTaxInvoice",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetIssuedTaxInvoice"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/issued-tax-
invoice/*"
    },
    {
      "Sid" : "AWSMarketplaceAgreementsCancellationAndAdjustmentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementInvoiceLineItems",
        "aws-marketplace:ListBillingAdjustmentRequests",
        "aws-marketplace:GetBillingAdjustmentRequest",
        "aws-marketplace:BatchCreateBillingAdjustmentRequest",
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest",
        "aws-marketplace:SendAgreementCancellationRequest",
        "aws-marketplace:CancelAgreementCancellationRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "TaxComplianceProfileChangeTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartTaxComplianceProfileChangeTask"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:tax-compliance-profile-change-task/*"
    },
    {
      "Sid" : "TaxComplianceProfileRead",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetTaxComplianceProfile"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:tax-compliance-profile/*"
    },
    {
      "Sid" : "TaxComplianceProfileList",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTaxComplianceProfileChangeTasks",
        "aws-marketplace:ListTaxComplianceProfiles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceSellerOfferManagement

Descrizione: fornisce ai venditori l'accesso alle attività di gestione di offerte e accordi.

`AWSMarketplaceSellerOfferManagement`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceSellerOfferManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 novembre 2024, 00:41 UTC
- Ora modificata: 31 marzo 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerOfferManagement`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOfferManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
```

```
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceCreateOfferOnProduct",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : "CreateOfferOnProduct"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceListEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntitiesReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ContainerProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProfessionalServicesProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/SaaSProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AmiProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceAgreementsCancellationAndAdjustmentReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementInvoiceLineItems",
        "aws-marketplace:ListBillingAdjustmentRequests",
        "aws-marketplace:GetBillingAdjustmentRequest",
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceSellerProductsFullAccess

Descrizione: fornisce ai venditori l'accesso completo alla pagina AWS Marketplace dei prodotti di gestione e ad altri AWS servizi come la gestione AMI.

`AWSMarketplaceSellerProductsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceSellerProductsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 luglio 2019, 21:06 UTC
- Ora modificata: 19 febbraio 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListAssessments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceAssessmentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeAssessment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetIAMRoleAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsightsAccess",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "ResourceSharingAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-files/
${aws:PrincipalAccount}/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "TechnicalStaff"
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMarketplaceSellerProductsReadOnly

Descrizione: fornisci ai venditori l'accesso in sola lettura alla pagina dei prodotti di AWS Marketplace gestione.

`AWSMarketplaceSellerProductsReadOnly`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSMarketplaceSellerProductsReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 luglio 2019, 21:40 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMcpServiceActionsFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni del servizio MCP. Questa politica non concede l'accesso alle azioni intraprese dall'MCP, ma solo alle azioni MCP stesse.

`AWSMcpServiceActionsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMcpServiceActionsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 novembre 2025, 22:49 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMcpServiceActionsFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllMCPServiceActions",
      "Effect" : "Allow",
      "Action" : "*",
```

```
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMCPSignInOAuthAccessPolicy

Descrizione: fornisce l'accesso per l'autenticazione al server AWS MCP tramite OAuth AWS Sign-In

`AWSMCPSignInOAuthAccessPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSMCPSignInOAuthAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 luglio 2026, 06:57 UTC
- Ora modificata: 09 luglio 2026, 06:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMCPSignInOAuthAccessPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOAuthForAWSMCP",
      "Effect" : "Allow",
      "Action" : [
        "signin:AuthorizeOAuth2Access",
        "signin:CreateOAuth2Token"
      ],
      "Resource" : "arn:aws:signin:*:*:service-principal/aws-mcp.amazonaws.com"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMediaConnectServicePolicy

Descrizione: la politica predefinita che consente l'accesso Servizi AWS e le risorse utilizzate o gestite da MediaConnect.

`AWSMediaConnectServicePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 3 aprile 2023 22:11 UTC
- Ora modificata: 29 ottobre 2025, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService",
        "ecs:CreateService",
        "ecs:DescribeServices",
        "ecs:PutAttributes",
        "ecs:DeleteAttributes",
        "ecs:RunTask",
        "ecs:ListTasks",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:UpdateClusterSettings",
        "ecs:ListAttributes",
        "ecs:DescribeClusters",
        "ecs:DeregisterContainerInstance",
        "ecs:ListContainerInstances"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/created-for-service" : "MediaConnect"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMediaLiveAnywhereServiceRolePolicy

Descrizione: consente a MediaLive Anywhere di creare e gestire AWS risorse per tuo conto.

`AWSMediaLiveAnywhereServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 aprile 2025, 22:07 UTC
- Ora modificata: 14 aprile 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaLiveAnywhereServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PutMediaLiveMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MediaLive"
        }
      }
    },
    {
      "Sid" : "RegisterAnywhereAgentTaskDefinition",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        }
      }
    },
    {
      "Sid" : "ECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : "RegisterTaskDefinition",
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "created_by"
        }
      }
    },
    {
      "Sid" : "UpdateAnywhereAgentService",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*",
          "ecs:Task-Definition" : "arn:aws:ecs:*:*:task-definition/
MediaLiveAnywhereAgent*"
        }
      }
    },
    {
      "Sid" : "ECSListTaskDefinitions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTaskDefinitions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeregisterAnywhereAgentTaskDefinitionOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeregisterTaskDefinition"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentTaskDefinitionsOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteTaskDefinitions"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentServiceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:service/MediaLiveAnywhere*/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
        }
      }
    },
    {
      "Sid" : "DeregisterContainerInstanceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListContainerInstances",
        "ecs:DeregisterContainerInstance"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMediaTailorServiceRolePolicy

Descrizione: Abilita l'accesso alle AWS risorse utilizzate o gestite da MediaTailor

`AWSMediaTailorServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 settembre 2021, 22:27 UTC
- Ora modificata: 17 settembre 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubDiscoveryAccess

Descrizione: la politica AWSMigration HubService consente di chiamare per AWSApplication DiscoveryService conto del cliente.

`AWSMigrationHubDiscoveryAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubDiscoveryAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 13:30 UTC

- Ora modificata: 6 agosto 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubDMSAccess

Descrizione: Politica per l'assunzione del ruolo del Database Migration Service nell'account del cliente per chiamare Migration Hub

`AWSMigrationHubDMSAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubDMSAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 14:00 UTC
- Ora modificata: 07 ottobre 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
```

```
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubFullAccess

Descrizione: policy gestita per fornire al cliente l'accesso al servizio Migration Hub

`AWSMigrationHubFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 agosto 2017, 14:02 UTC
- Ora modificata: 19 giugno 2019, 21:14 UTC

- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubOrchestratorConsoleFullAccess

Descrizione: fornisce un accesso limitato a AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service e AWS Secrets Manager. Questa politica garantisce inoltre l'accesso completo al servizio AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorConsoleFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubOrchestratorConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 aprile 2022, 02:26 UTC
- Ora modificata: 05 dicembre 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHO",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
```

```
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3MHO",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Configuration",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations",
        "discovery:GetDiscoverySummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetHomeRegion",
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListProfileRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Account",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CreateServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "migrationhub-orchestrator.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
orchestrator.amazonaws.com/AWSServiceRoleForMigrationHubOrchestrator*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubOrchestratorInstanceRolePolicy

Descrizione: questa policy deve essere allegata per le istanze migrate da SAP e MGN per consentire al nostro servizio di orchestrare le istanze scaricando script da S3 e recuperare valori segreti all'interno dell'istanza EC2.

`AWSMigrationHubOrchestratorInstanceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubOrchestratorInstanceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 aprile 2022, 02:43 UTC
- Ora modificata: 20 aprile 2022, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubOrchestratorPlugin

Descrizione: fornisce un accesso limitato alle azioni relative ad Amazon Simple Storage Service, AWS Secrets Manager e Plugin per AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorPlugin`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubOrchestratorPlugin` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 aprile 2022, 02:25 UTC
- Ora modificata: 20 aprile 2022, 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:RegisterPlugin",
        "migrationhub-orchestrator:GetMessage",
        "migrationhub-orchestrator:SendMessage"
```

```
      ],
      "Resource" : "arn:aws:migrationhub-orchestrator:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubOrchestratorServiceRolePolicy

Descrizione: Fornisce le autorizzazioni necessarie a Migration Hub Orchestrator per migrare e modernizzare i carichi di lavoro locali

`AWSMigrationHubOrchestratorServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 aprile 2022, 02:24 UTC
- Ora modificata: 4 marzo 2024, 18:25 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationDiscoveryService",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchWizard",
      "Effect" : "Allow",
      "Action" : [
        "launchwizard:ListProvisionedApps",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:ListDeployments",
        "launchwizard:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ec2MGNLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ec2LaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "getHomeRegion",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMcommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "ssm:CancelCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*",
```

```
        "arn:aws:s3:::migrationhub-orchestrator-*"
      ]
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "s3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:DeleteRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/MigrationHubOrchestratorManagedRule*"
    },
    {
      "Sid" : "MGN",
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetReplicationConfiguration",
        "mgn:GetLaunchConfiguration",
        "mgn:StartCutover",
```

```
        "mgn:FinalizeCutover",
        "mgn:StartTest",
        "mgn:UpdateReplicationConfiguration",
        "mgn:DescribeSourceServers",
        "mgn:MarkAsArchived",
        "mgn:ChangeServerLifeCycleState"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2DescribeImportImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImportImageTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "s3ListBucket",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "migrationhub-orchestrator-vmie-*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

Descrizione: concede l'accesso completo a AWS Migration Hub Refactor Spaces e ad altri servizi AWS correlati ad eccezione dei gruppi di sicurezza AWS Transit Gateway e EC2 non richiesti quando si utilizzano ambienti senza un bridge di rete. Questa politica esclude anche le autorizzazioni richieste per AWS Lambda e AWS Resource Access Manager in quanto possono essere delimitate in base ai tag.

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 aprile 2023, 20:09 UTC
- Ora modificata: 11 aprile 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsDelete",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationDelete",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
```

```
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Sid" : "ELBListenerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBListenerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackTag",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid" : "CreateRefactorSpacesSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "CreateELBSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Descrizione: utilizzo nel ruolo di servizio IAM passato al documento di automazione SSM AWSRefactorSpaces-CreateResources per concedere le autorizzazioni necessarie per eseguire l'automazione. La policy consente l' read/write accesso ai tag EC2 per tenere traccia dei progressi dell'automazione. Quando il bridge di rete dell'ambiente Refactor Spaces è abilitato, l'automazione aggiunge anche il gruppo di sicurezza dell'ambiente all'istanza EC2 per consentire il traffico proveniente da altri servizi Refactor Spaces presenti nell'ambiente. La policy consente inoltre l'accesso ai parametri SSM delle azioni successive al lancio dell'Application Migration Service.

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 agosto 2023, 15:08 UTC
- Ora modificata: 10 agosto 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "refactor-spaces:ssm:environment-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubRefactorSpacesFullAccess

Descrizione: concede l'accesso completo a AWS MigrationHub Refactor Spaces, alle funzionalità della console di AWS MigrationHub Refactor Spaces e ad altri AWS servizi correlati, ad eccezione delle autorizzazioni richieste per Lambda e AWS Resource Access AWS Manager in quanto possono essere delimitate in base ai tag.

`AWSMigrationHubRefactorSpacesFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubRefactorSpacesFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2021, 07:12 UTC
- Ora modificata: 11 aprile 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RequestTagTransitGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "ResourceTagTransitGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2NetworkingModify",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTransitGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "ELBLoadBalancerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Sid" : "ELBListenerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBListenerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
```

```
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
```

```
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackTag",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid" : "CreateRefactorSpacesSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateELBSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubRefactorSpacesServiceRolePolicy

Descrizione: fornisce l'accesso alle AWS risorse gestite o utilizzate da AWS Migration Hub Refactor Spaces.

`AWSMigrationHubRefactorSpacesServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 29 novembre 2021, 06:50 UTC
- Ora modificata: 20 luglio 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PUT",
        "apigateway:POST",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
```

```
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/vpclinks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubSMSAccess

Descrizione: Politica per l'assunzione del ruolo del servizio di migrazione dei server nell'account del cliente per chiamare Migration Hub

`AWSMigrationHubSMSAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubSMSAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 agosto 2017, 13:57 UTC
- Ora modificata: 07 ottobre 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Action" : [
```

```
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubStrategyCollector

Descrizione: concede le autorizzazioni per consentire la comunicazione con il servizio AWS Migration Hub Strategy Recommendations, read/write l'accesso ai bucket S3 relativi al servizio, l'accesso ad Amazon API Gateway su cui caricare log e metriche, l'accesso a AWS Secrets AWS Manager per recuperare le credenziali e tutti i servizi correlati.

`AWSMigrationHubStrategyCollector`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubStrategyCollector` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 ottobre 2021, 20:15 UTC
- Ora modificata: 01 aprile 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:GetBucketLocation"
```

```
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowS3ListBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowMetricsAndLogs",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:PutMetricData",
        "application-transformation:PutLogData",
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MHSRAllowExecuteAPI",
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
```

```
      ]
    },
    {
      "Sid" : "MHSRAllowCollectorAPI",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:RegisterCollector",
        "migrationhub-strategy:GetAntiPattern",
        "migrationhub-strategy:GetMessage",
        "migrationhub-strategy:SendMessage",
        "migrationhub-strategy:ListAntiPatterns",
        "migrationhub-strategy:ListJarArtifacts",
        "migrationhub-strategy:UpdateCollectorConfiguration",
        "migrationhub-strategy:PutLogData",
        "migrationhub-strategy:PutMetricData"
      ],
      "Resource" : "arn:aws:migrationhub-strategy:*:*:*"
    },
    {
      "Sid" : "MHSRAllowSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubStrategyConsoleFullAccess

Descrizione: concede l'accesso completo al servizio AWS Migration Hub Strategy Recommendations e l'accesso ai AWS servizi correlati tramite. Console di gestione AWS

`AWSMigrationHubStrategyConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMigrationHubStrategyConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 ottobre 2021, 20:13 UTC
- Ora modificata: 09 novembre 2022, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:GetDiscoverySummary",
        "discovery:DescribeTags",
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "migrationhub-strategy.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
strategy.amazonaws.com/AWSMigrationHubStrategyServiceRolePolicy*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMigrationHubStrategyServiceRolePolicy

Descrizione: Abilita l'accesso alle AWS risorse utilizzate o gestite dal servizio AWS Migration Hub Strategy Recommendations.

`AWSMigrationHubStrategyServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 ottobre 2021, 20:02 UTC

- Ora modificata: 19 ottobre 2021, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "permissionsForAds",
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "permissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
```

```
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMobileHub_FullAccess

Descrizione: questa politica può essere allegata a qualsiasi utente, ruolo o gruppo, al fine di concedere agli utenti l'autorizzazione a creare, eliminare e modificare progetti (e le AWS risorse associate) in AWS Mobile Hub. Ciò include anche le autorizzazioni per generare e scaricare codice sorgente di app mobili di esempio per ogni progetto Mobile Hub.

`AWSMobileHub_FullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMobileHub_FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 gennaio 2016, 19:56 UTC
- Ora modificata: 19 dicembre 2019, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "cloudfront:GetDistribution",
        "devicefarm:CreateProject",
        "devicefarm:ListJobs",
        "devicefarm:ListRuns",
        "devicefarm:GetProject",
        "devicefarm:GetRun",
        "devicefarm:ListArtifacts",
        "devicefarm:ListProjects",
        "devicefarm:ScheduleRun",
        "dynamodb:DescribeTable",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMobileHub_ReadOnly

Descrizione: questa politica può essere allegata a qualsiasi Utente, Ruolo o Gruppo, al fine di concedere agli utenti l'autorizzazione a elencare e visualizzare i progetti in AWS Mobile Hub. Ciò include anche le autorizzazioni per generare e scaricare codice sorgente di app mobili di esempio per ogni progetto Mobile Hub. Non consente all'utente di modificare alcuna configurazione per alcun progetto Mobile Hub.

`AWSMobileHub_ReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSMobileHub_ReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 gennaio 2016, 19:55 UTC
- Ora modificata: 23 luglio 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:ExportProject",
```

```
        "mobilehub:GenerateProjectParameters",
        "mobilehub:GetProject",
        "mobilehub:SynchronizeProject",
        "mobilehub:GetProjectSnapshot",
        "mobilehub:ListProjectSnapshots",
        "mobilehub:ListAvailableConnectors",
        "mobilehub:ListAvailableFeatures",
        "mobilehub:ListAvailableRegions",
        "mobilehub:ListProjects",
        "mobilehub:ValidateProject",
        "mobilehub:VerifyServiceRole",
        "mobilehub:DescribeBundle",
        "mobilehub:ExportBundle",
        "mobilehub:ListBundles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSMSKReplicatorExecutionRole

Descrizione: concede le autorizzazioni ad Amazon MSK Replicator per replicare i dati tra cluster MSK.

`AWSMSKReplicatorExecutionRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSMSKReplicatorExecutionRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 06 dicembre 2023, 00:07 UTC
- Ora modificata: 25 marzo 2024, 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
```

```
        "kafka-cluster:WriteDataIdempotently"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "TopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:AlterCluster"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:topic/*/*"
      ]
    },
    {
      "Sid" : "GroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:group/*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSNATGatewayServiceRolePolicy

Descrizione: fornisce le autorizzazioni per gestire le risorse VPC per la configurazione e la gestione dei gateway NAT.

`AWSNATGatewayServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 novembre 2025, 17:19 UTC
- Ora modificata: 14 novembre 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNATGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSNetworkFirewallFullAccess

Descrizione: concede l'accesso completo al servizio AWS Network Firewall, incluse le autorizzazioni per creare, configurare, gestire ed eliminare risorse, politiche e gruppi di regole del firewall. Include inoltre le autorizzazioni per modificare gli endpoint VPC, le policy dei bucket S3, le configurazioni dei log e la creazione di CloudWatch ruoli collegati ai servizi per Network Firewall e i servizi di consegna dei log

`AWSNetworkFirewallFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSNetworkFirewallFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 giugno 2025, 21:52 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:CreateRuleGroup",
        "network-firewall:CreateTLSInspectionConfiguration",
        "network-firewall:DeleteFirewall",
```

```
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DeleteRuleGroup",
        "network-firewall:DeleteTLSInspectionConfiguration",
        "network-firewall:DisassociateSubnets",
        "network-firewall:PutResourcePolicy",
        "network-firewall:StartAnalysisReport",
        "network-firewall:StartFlowCapture",
        "network-firewall:StartFlowFlush",
        "network-firewall:UpdateFirewallAnalysisSettings",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallDescription",
        "network-firewall:UpdateFirewallEncryptionConfiguration",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:UpdateRuleGroup",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:UpdateTLSInspectionConfiguration"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*"
      ]
    },
    {
      "Sid" : "NetworkFirewallEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallDeleteVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLogging",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallLoggingCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallLoggingS3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLoggingFirehose",
      "Effect" : "Allow",
      "Action" : "firehose:TagDeliveryStream",
      "Resource" : "arn:aws:firehose:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/network-firewall.amazonaws.com/
AWSServiceRoleForNetworkFirewall"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network-firewall.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSNetworkFirewallReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura alle risorse del AWS Network Firewall tramite, Console di gestione AWS CLI e. SDKs Questa politica consente agli utenti di visualizzare e monitorare le configurazioni del firewall, le politiche, i gruppi di regole e le risorse associate, senza la possibilità di apportare modifiche.

`AWSNetworkFirewallReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSNetworkFirewallReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 giugno 2025, 21:52 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListProxies",
        "network-firewall:ListProxyConfigurations",
        "network-firewall:ListProxyRuleGroups",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListVpcEndpointAssociations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeProxy",
        "network-firewall:DescribeProxyConfiguration",
        "network-firewall:DescribeProxyRule",
        "network-firewall:DescribeProxyRuleGroup",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:DescribeVpcEndpointAssociation",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults"
      ],
      "Resource" : "arn:aws:network-firewall:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSNetworkFirewallServiceRolePolicy

Descrizione: consente AWSNetworkFirewall di creare e gestire le risorse necessarie per i firewall.

`AWSNetworkFirewallServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 17 novembre 2020, 17:17 UTC
- Ora modificata: 01 giugno 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "acm:DescribeCertificate",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroupResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "resource-groups.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*",
        "arn:aws:ecs:*:*:container-instance/*/*",
        "arn:aws:ecs:*:*:task/*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSNetworkManagerCloudWANServiceRolePolicy

Descrizione: consente NetworkManager di accedere alle risorse associate alla rete principale

`AWSNetworkManagerCloudWANServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 luglio 2022, 12:17 UTC
- Ora modificata: 12 luglio 2022, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
```

```
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSNetworkManagerFullAccess

Descrizione: fornisce l'accesso completo ad Amazon NetworkManager tramite Console di gestione AWS.

`AWSNetworkManagerFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSNetworkManagerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 17:37 UTC
- Ora modificata: 03 dicembre 2019, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSNetworkManagerReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ad Amazon NetworkManager tramite Console di gestione AWS.

`AWSNetworkManagerReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSNetworkManagerReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 dicembre 2019, 17:35 UTC
- Ora modificata: 03 dicembre 2019, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:Describe*",
        "networkmanager:Get*",
        "networkmanager:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSNetworkManagerServiceRolePolicy

Descrizione: consenti l'accesso NetworkManager alle risorse associate alle tue reti globali

`AWSNetworkManagerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 03 dicembre 2019, 14:03 UTC
- Ora modificata: 27 luglio 2022, 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeLocations",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpcs",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeRegions",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSObservabilityAdminLogsCentralizationServiceRolePolicy

Descrizione: autorizzazioni di ruolo collegate al servizio per la centralizzazione dei registri CloudWatch

`AWSObservabilityAdminLogsCentralizationServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 settembre 2025, 14:34 UTC
- Ora modificata: 15 settembre 2025, 14:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminLogsCentralizationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "logs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/LogsManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:logs:arn" : "arn:aws:logs:*:*:log-group:*"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSObservabilityAdminServiceRolePolicy

Descrizione: fornisce l'accesso per gestire AWS Config Configuration Recorder, gestire Config Configuration Aggregator, creare la funzionalità AWS AWS Config Service Linked Role for Configuration Recorder, utilizzare i dati di configurazione del registratore e leggere i dati delle organizzazioni per le funzionalità organizzative. AWS

`AWSObservabilityAdminServiceRolePolicy`è una policy gestita. AWS

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 27 novembre 2024, 19:36 UTC
- Ora modificata: 14 luglio 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminServiceRolePolicy`

Versione della politica

Versione della politica: v2 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator",
        "config:DeleteConfigurationAggregator",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
observabilityadmin.amazonaws.com/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "observabilityadmin.amazonaws.com",
            "config.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy

Descrizione: fornisce l'accesso per gestire le risorse del registratore di AWS Config e le impostazioni di telemetria sulle AWS risorse, inclusi registri e metriche.

`AWSObservabilityAdminTelemetryEnablementServiceRolePolicy`è AWS una policy gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 01 agosto 2025, 18:04 UTC
- Ora modificata: 24 luglio 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminTelemetryEnablementServiceRolePolicy`

Versione della politica

Versione della politica: v14 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TelemetryOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeFlowLogs",
        "ec2:DescribeVpcs",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:ListLogGroups",
        "ec2:MonitorInstances",
        "logs:DescribeDeliverySources",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOperationForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        },
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateFlowLogs"
        }
      }
```

```
    },
    {
      "Sid" : "TagOperationForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCFlowLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-flow-log/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        },
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteFlowLogs",
        "logs:CreateDelivery",
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliverySource",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSApiLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/api" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuditLogs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/audit" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuthenticatorLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/authenticator" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSControllerManagerLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/controllerManager" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSSchedulerLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/scheduler" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLoggingConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "arn:aws:wafv2:*:*:*/webacl/*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:logs:*:*:log-group:*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "wafv2:LogScope" : "CloudwatchTelemetryRuleManaged"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:AllowVendedLogDeliveryForResource",
        "bedrock:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForSecurityHub",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:AllowVendedLogDeliveryForResource",
        "securityhub:DescribeHub",
        "securityhub:DescribeSecurityHubV2"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForCloudfront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForCloudTrailLogs",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/cloudwatch/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForManagedLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/cloudtrail",
        "arn:aws:logs:*:*:log-group:aws/cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingListOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListTagsForResource"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingConfigCreation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:CreateResolverQueryLogConfig",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:resolver-query-log-config/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingConfigAssociation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateResolverQueryLogConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/route53resolver.amazonaws.com/
AWSServiceRoleForRoute53Resolver",
```

```
      "Condition" : {
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : [
            "route53resolver.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMOperationsForConfigServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManagementOperationsForServiceLinkedRecorder",
```

```
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin_TelemetryEnablement/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadOperationsForServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "config:ConfigurationRecorderServicePrincipal" : [
            "telemetry-enablement.observabilityadmin.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForKafka",
      "Effect" : "Allow",
      "Action" : [
        "kafka:UpdateMonitoring",
        "kafka:DescribeCluster"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentSimba",
      "Effect" : "Allow",
      "Action" : [
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:StartTelemetryEnrichment",
        "observabilityadmin:StopTelemetryEnrichment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentResourceExplorer",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateManagedView",
        "resource-explorer-2:CreateStreamingAccessForService",
        "resource-explorer-2:DeleteStreamingAccessForService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetOTelEnrichment",
```

```
        "cloudwatch:StartOTelEnrichment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "iam:AWSServiceName" : "resource-explorer-2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TelemetryReadTagsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryKMSOperationsForAccount",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:Describe*",
        "logs:AssociateKmsKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryKMSOperationsForOrganization",
      "Effect" : "Allow",
      "Action" : [
        "kms:Describe*",
        "logs:AssociateKmsKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalOrgId" : "${aws:ResourceOrgId}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSOrganizationsFullAccess

Descrizione: Fornisce l'accesso completo a AWS Organizations.

`AWSOrganizationsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSOrganizationsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 novembre 2018, 20:31 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account:DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion",
        "account:PutAccountName",
        "account:GetAccountInformation"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSOrganizationsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a Organizations AWS .

`AWSOrganizationsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSOrganizationsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 novembre 2018, 20:32 UTC

- Ora modificata: 07 giugno 2024, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "account:GetPrimaryEmail"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSOrganizationsServiceTrustPolicy

Descrizione: una politica per consentire alle AWS Organizzazioni di condividere la fiducia con altri, approvata allo Servizi AWS scopo di semplificare la configurazione del cliente.

`AWSOrganizationsServiceTrustPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 ottobre 2017, 23:04 UTC
- Ora modificata: 5 marzo 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForOrganizations",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/organizations.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesSLR",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSOutpostsAuthorizeServerPolicy

Descrizione: questa politica concede le autorizzazioni che consentono di installare un server Outpost sulla rete locale.

`AWSOutpostsAuthorizeServerPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSOutpostsAuthorizeServerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 gennaio 2023, 19:23 UTC
- Ora modificata: 04 gennaio 2023, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSOutpostsServiceRolePolicy

Descrizione: policy Service Linked Role per consentire l'accesso alle AWS risorse gestite da AWS Outposts

`AWSOutpostsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 09 novembre 2020, 22:55 UTC
- Ora modificata: 17 aprile 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "PrivateConnectivityServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfacePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfaceTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
```

```
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPanoramaApplianceRolePolicy

Descrizione: consente al software AWS IoT su un'appliance AWS Panorama di caricare i log su Amazon. CloudWatch

`AWSPanoramaApplianceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPanoramaApplianceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2020, 13:13 UTC
- Ora modificata: 01 dicembre 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*"
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPanoramaApplianceServiceRolePolicy

Descrizione: consente a un'appliance AWS Panorama di caricare log su Amazon CloudWatch e di ottenere oggetti dai punti di accesso Amazon S3 creati per l'uso con Panorama. AWS

`AWSPanoramaApplianceServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSPanoramaApplianceServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 ottobre 2021, 12:14 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDevicePutMetric",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "PanoramaDeviceMetrics"
        }
      }
    },
    {
      "Sid" : "PanoramaDeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:ListBucket",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*-nodepackage-store-*",
        "arn:aws:s3:::*-application-payload-store-*",
        "arn:aws:s3:*:*:accesspoint/panorama*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPanoramaFullAccess

Descrizione: Fornisce accesso completo a AWS Panorama

`AWSPanoramaFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPanoramaFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2020, 13:12 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "panorama.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "panorama.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPanoramaGreengrassGroupRolePolicy

Descrizione: consente a una funzione AWS Lambda su un dispositivo AWS Panorama di gestire le risorse in Panorama, caricare log e metriche su Amazon e gestire oggetti in CloudWatch bucket creati per l'uso con Panorama.

`AWSPanoramaGreengrassGroupRolePolicy`[è una politica gestita.AWS]

Utilizzo di questa politica

È possibile associare la policy `AWSPanoramaGreengrassGroupRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2020, 13:10 UTC
- Ora modificata: 6 gennaio 2021, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
```

```
        "s3:GetBucket*",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCLoudWatchPutDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "PanoramaGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPanoramaSageMakerRolePolicy

Descrizione: consente SageMaker ad Amazon di gestire oggetti in bucket creati per l'uso con AWS Panorama.

`AWSPanoramaSageMakerRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPanoramaSageMakerRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2020, 13:13 UTC
- Ora modificata: 01 dicembre 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPanoramaServiceLinkedRolePolicy

Descrizione: consente a AWS Panorama di gestire le risorse in AWS IoT, AWS Secrets Manager e AWS Panorama.

`AWSPanoramaServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 ottobre 2021, 12:12 UTC
- Ora modificata: 20 ottobre 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyAndVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:AttachPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
```

```
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPanoramaServiceRolePolicy

Descrizione: consente a AWS Panorama di gestire le risorse in Amazon S3, AWS AWS IoT, GreenGrass AWS Lambda SageMaker, Amazon e CloudWatch Amazon Logs e di trasferire i ruoli di servizio a IoT, AWS AWS GreenGrass IoT e Amazon. SageMaker

`AWSPanoramaServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSPanoramaServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 dicembre 2020, 13:14 UTC
- Ora modificata: 01 dicembre 2020, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*",
        "panorama:Get*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaSageMakerRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaSageMakerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/AWSPanoramaGreengrassRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassRole"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassIoTRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PanoramaGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
```

```
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteResourceDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
```

```
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:StopCompilationJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/panorama*",
        "arn:aws:sagemaker:*:*:compilation-job/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:ListCompilationJobs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "PanoramaCWLogsAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:CreateRoleAlias"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*",
        "arn:aws:iot:*:*:rolealias/panorama*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerCentralChannelHandshakeApprovalManagement

Descrizione: fornisce l'accesso necessario per le attività di gestione dell'approvazione dell'handshake del canale.

`AWSPartnerCentralChannelHandshakeApprovalManagement`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerCentralChannelHandshakeApprovalManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 novembre 2025, 16:34 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralChannelHandshakeApprovalManagement`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelHandshakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListChannelHandshakes",
        "partnercentral:AcceptChannelHandshake",
```

```
        "partnercentral:RejectChannelHandshake"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerCentralChannelManagement

Descrizione: fornisce l'accesso necessario per le attività di gestione dei canali.

`AWSPartnerCentralChannelManagement`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerCentralChannelManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 novembre 2025, 16:34 UTC
- Ora modificata: 14 febbraio 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralChannelManagement`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateProgramManagementAccount",
        "partnercentral:UpdateProgramManagementAccount",
        "partnercentral:DeleteProgramManagementAccount",
        "partnercentral:ListProgramManagementAccounts",
        "partnercentral:GetProgramManagementAccount",
        "partnercentral:CreateRelationship",
        "partnercentral:UpdateRelationship",
        "partnercentral:DeleteRelationship",
        "partnercentral:GetRelationship",
        "partnercentral:ListRelationships",
        "partnercentral:CreateChannelHandshake",
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake",
        "partnercentral:CancelChannelHandshake",
        "partnercentral:ListChannelHandshakes"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/program-management-account/*",
        "arn:aws:partnercentral:*:*:catalog/*/channel-handshake/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "ChannelUser"
        }
      }
```

```
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Resell_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerCentralFullAccess

Descrizione: Fornisce l'accesso completo a AWS Partner Central e ai servizi correlati Servizi AWS.

`AWSPartnerCentralFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerCentralFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 novembre 2024, 23:33 UTC
- Ora modificata: 12 marzo 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralFullAccess`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "PassAWSPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "Partnercentral-account-management:AssociatePartnerUser",
        "Partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "VerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartVerification",
        "partnercentral:GetVerification"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
```

```
      ]
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "SupportAccess",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase",
        "support:AddAttachmentsToSet",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListEntitiesAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
```

```
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
```

```
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerCentralMarketingManagement

Descrizione: fornisce l'accesso necessario per le attività di marketing.

`AWSPartnerCentralMarketingManagement`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerCentralMarketingManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2025, 00:34 UTC
- Ora modificata: 14 febbraio 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralMarketingManagement`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "MarketingStaff"
        }
      }
    },
    {
      "Sid" : "PartnerDiscoveryAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:SearchPartnerProfiles",
        "partnercentral:GetPartnerProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartProfileUpdateTask",
        "partnercentral:GetProfileUpdateTask",
        "partnercentral:CancelProfileUpdateTask",
```

```
        "partnercentral:PutProfileVisibility",
        "partnercentral:GetProfileVisibility"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
```

```
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/MarketingCampaign_V1/
Dashboard/*"
      ]
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerCentralOpportunityManagement

Descrizione: fornisce l'accesso necessario per le attività di gestione delle opportunità.

`AWSPartnerCentralOpportunityManagement`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerCentralOpportunityManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 novembre 2024, 19:09 UTC
- Ora modificata: 16 giugno 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralOpportunityManagement`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpportunityManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:AcceptEngagementInvitation",
        "partnercentral:AssignOpportunity",
        "partnercentral:AssociateOpportunity",
        "partnercentral:CreateEngagement",
        "partnercentral:CreateEngagementContext",
        "partnercentral:CreateEngagementInvitation",
        "partnercentral:CreateOpportunity",
        "partnercentral:CreateResourceSnapshot",
        "partnercentral:CreateResourceSnapshotJob",
        "partnercentral:DeleteResourceSnapshotJob",
        "partnercentral:DisassociateOpportunity",
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetEngagement",
        "partnercentral:GetEngagementInvitation",
        "partnercentral:GetOpportunity",
        "partnercentral:GetProspectingFromEngagementTask",
```

```
        "partnercentral:GetResourceSnapshot",
        "partnercentral:GetResourceSnapshotJob",
        "partnercentral:ListEngagementByAcceptingInvitationTasks",
        "partnercentral:ListEngagementFromOpportunityTasks",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagementMembers",
        "partnercentral:ListEngagementResourceAssociations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListOpportunityFromEngagementTasks",
        "partnercentral:ListProspectingFromEngagementTasks",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "partnercentral:ListSolutions",
        "partnercentral:RejectEngagementInvitation",
        "partnercentral:StartEngagementByAcceptingInvitationTask",
        "partnercentral:StartEngagementFromOpportunityTask",
        "partnercentral:StartOpportunityFromEngagementTask",
        "partnercentral:StartProspectingFromEngagementTask",
        "partnercentral:StartResourceSnapshotJob",
        "partnercentral:StopResourceSnapshotJob",
        "partnercentral:SubmitOpportunity",
        "partnercentral:UpdateEngagementContext",
        "partnercentral:UpdateOpportunity"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AWSMarketplaceEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "AceManager"
        }
      }
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Opportunity_V1/Dashboard/
*",
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Engagement_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "CollaborationChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateCollaborationChannelRequest",
        "partnercentral:ListCollaborationChannels",
        "partnercentral:GetCollaborationChannel",
        "partnercentral:CreateCollaborationChannelMembers"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/*/resource-snapshot-job/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerCentralRevenueAttributionManagement

Descrizione: fornisce l'accesso necessario per le attività di gestione dell'attribuzione dei ricavi.

`AWSPartnerCentralRevenueAttributionManagement`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerCentralRevenueAttributionManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 giugno 2026, 19:12 UTC
- Ora modificata: 30 giugno 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralRevenueAttributionManagement`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RevenueMeasurementCreation",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateRevenueAttribution",
        "partnercentral:CreateMarketplaceRevenueShare",
        "partnercentral:CreateMarketplaceRevenueShareAllocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
```

```
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueMeasurementListing",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListRevenueAttributions",
        "partnercentral:ListRevenueAttributionAllocations",
        "partnercentral:ListMarketplaceRevenueShares",
        "partnercentral:ListMarketplaceRevenueShareAllocations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueAttributionManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetRevenueAttribution",
        "partnercentral:UpdateRevenueAttribution",
        "partnercentral:GetRevenueAttributionAllocation",
        "partnercentral:StartRevenueAttributionAllocationsTask",
        "partnercentral:GetRevenueAttributionAllocationsTask"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "MarketplaceRevenueShareManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetMarketplaceRevenueShare",
        "partnercentral:GetMarketplaceRevenueShareAllocation",
        "partnercentral:UpdateMarketplaceRevenueShareAllocation"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/marketplace-revenue-share/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
        "arn:aws:partnercentral:*:*:catalog/*/marketplace-revenue-share/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "OpportunityListing",
      "Effect" : "Allow",
      "Action" : [
```

```
        "partnercentral:ListOpportunities"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "OpportunityAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetOpportunity"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerListing",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartner"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerCentralSandboxFullAccess

Descrizione: fornisce l'accesso necessario per i test degli sviluppatori nel catalogo Sandbox.

`AWSPartnerCentralSandboxFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerCentralSandboxFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 novembre 2024, 19:10 UTC
- Ora modificata: 12 marzo 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSandboxFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSPartnerCentralSandboxAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        }
      }
    },
    {
      "Sid" : "PartnerCentralAgentsSandboxSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy

Descrizione: fornisce l'accesso ResourceSnapshotJob alla lettura di una risorsa e alla relativa istantanea nel coinvolgimento target.

`AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 dicembre 2024, 18:21 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateResourceSnapshot"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*::catalog/AWS/engagement/*",
        "arn:aws:partnercentral:*::catalog/Sandbox/engagement/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetOpportunity"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/AWS/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/Sandbox/opportunity/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerLedSupportReadOnlyAccess

Descrizione: questo criterio può essere utilizzato per concedere l'accesso in sola lettura ai metadati di servizio in APIs grado di leggere per i servizi del tuo. Account AWS Puoi utilizzare questa politica per fornire ai tuoi partner del Partner-Led Support Program l'accesso ai servizi specificati nella sezione dei dettagli delle autorizzazioni di seguito.

`AWSPartnerLedSupportReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerLedSupportReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 novembre 2024, 20:06 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerLedSupportReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
```

```
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
```

```
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
```

```
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupPlans",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listLegalHolds",
```

```
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeStacks",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listStacks",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypeVersions",
        "cloudformation:listTypes",
        "cloudfront:describeFunction",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
```

```
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
```

```
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetricStreams",
        "cloudwatch:listMetrics",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineState",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getGroup",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
```

```
        "cognito-sync:listIdentityPoolUsage",
        "connect:describeContact",
        "connect:describePhoneNumber",
        "connect:describeQuickConnect",
        "connect:describeUser",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:listContactEvaluations",
        "connect:listEvaluationFormVersions",
        "connect:listEvaluationForms",
        "connect:listPhoneNumbersV2",
        "connect:listQuickConnects",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listUsers",
        "connect:listViewVersions",
        "connect:listViews",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEndpoints",
        "dms:describeEventCategories",
        "dms:describeEventSubscriptions",
        "dms:describeEvents",
        "dms:describeFleetAdvisorCollectors",
```

```
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationInstances",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddressTransfers",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
```

```
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdFormat",
        "ec2:describeIdentityIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInstances",
        "ec2:describeInternetGateways",
        "ec2:describeIpamPools",
        "ec2:describeIpamScopes",
        "ec2:describeIpams",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLaunchTemplates",
```

```
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeLocalGateways",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSnapshots",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
```

```
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeTransitGateways",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumeStatus",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
```

```
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getSubnetCidrReservations",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTaskSets",
        "ecs:describeTasks",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeNodegroup",
        "eks:describePodIdentityAssociation",
```

```
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
```

```
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
```

```
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
```

```
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
```

```
        "glue:getJob",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getMapping",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableVersions",
        "glue:getTables",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemaVersions",
        "glue:listSchemas",
        "glue:listSessions",
        "glue:listStatements",
```

```
        "glue:querySchemaVersionMetadata",
        "guardduty:getFindings",
        "guardduty:listDetectors",
        "guardduty:listFindings",
        "guardduty:listIPSets",
        "guardduty:listThreatIntelSets",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getSSHPublicKey",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
```

```
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listSSHPublicKeys",
        "iam:listServerCertificates",
        "iam:listSigningCertificates",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
```

```
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctionUrlConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listLayerVersions",
        "lambda:listLayers",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listVersionsByFunction",
        "logs:describeExportTasks",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeSubscriptionFilters",
        "medialive:listChannels",
        "medialive:listInputSecurityGroups",
        "medialive:listInputs",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
```

```
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "pipes:listPipes",
        "polly:describeVoices",
        "polly:listLexicons",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
```

```
        "quicksight:listAnalyses",
        "quicksight:listDashboardVersions",
        "quicksight:listDashboards",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplateVersions",
        "quicksight:listTemplates",
        "quicksight:listThemeAliases",
        "quicksight:listThemeVersions",
        "quicksight:listThemes",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBParameterGroups",
```

```
        "rds:describeDBParameters",
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEventSubscriptions",
        "rds:describeEvents",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterVersions",
```

```
        "redshift:describeClusters",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
        "redshift:describeEventSubscriptions",
        "redshift:describeEvents",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
```

```
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
```

```
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
```

```
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultiRegionAccessPoints",
        "s3:listMultipartUploadParts",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
        "s3express:listAllMyDirectoryBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
```

```
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
```

```
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubContents",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImageVersions",
        "sagemaker:listImages",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCardVersions",
```

```
            "sagemaker:listModelCards",
            "sagemaker:listModelExplainabilityJobDefinitions",
            "sagemaker:listModelMetadata",
            "sagemaker:listModelPackageGroups",
            "sagemaker:listModelPackages",
            "sagemaker:listModelQualityJobDefinitions",
            "sagemaker:listModels",
            "sagemaker:listMonitoringAlertHistory",
            "sagemaker:listMonitoringAlerts",
            "sagemaker:listMonitoringExecutions",
            "sagemaker:listMonitoringSchedules",
            "sagemaker:listNotebookInstanceLifecycleConfigs",
            "sagemaker:listNotebookInstances",
            "sagemaker:listPipelineExecutionSteps",
            "sagemaker:listPipelineExecutions",
            "sagemaker:listPipelineParametersForExecution",
            "sagemaker:listPipelines",
            "sagemaker:listProcessingJobs",
            "sagemaker:listProjects",
            "sagemaker:listSpaces",
            "sagemaker:listStageDevices",
            "sagemaker:listStudioLifecycleConfigs",
            "sagemaker:listSubscribedWorkteams",
            "sagemaker:listTags",
            "sagemaker:listTrainingJobs",
            "sagemaker:listTrainingJobsForHyperParameterTuningJob",
            "sagemaker:listTransformJobs",
            "sagemaker:listTrialComponents",
            "sagemaker:listTrials",
            "sagemaker:listUserProfiles",
            "sagemaker:listWorkforces",
            "sagemaker:listWorkteams",
            "scheduler:listScheduleGroups",
            "scheduler:listSchedules",
            "servicequotas:listAWSDefaultServiceQuotas",
            "servicequotas:listServiceQuotas",
            "ses:describeActiveReceiptRuleSet",
            "ses:describeConfigurationSet",
            "ses:describeReceiptRule",
            "ses:describeReceiptRuleSet",
            "ses:getAccount",
            "ses:getAccountSendingEnabled",
            "ses:getBlacklistReports",
            "ses:getConfigurationSet",
```

```
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listVerifiedEmailAddresses",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
```

```
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotationShifts",
        "ssm-contacts:listRotations",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listDatabases",
```

```
        "ssm-sap:listOperations",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAssociationExecutions",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInstancePatches",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroupState",
        "ssm:describePatchGroups",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
```

```
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociationVersions",
        "ssm:listAssociations",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocumentVersions",
        "ssm:listDocuments",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
```

```
        "vpc-lattice:listListeners",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
```

```
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
```

```
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeApplicationAssociations",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspacesConnectionStatus"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerProServeToolsFullAccess

Descrizione: fornisce l'accesso completo agli ProServe strumenti.

`AWSPartnerProServeToolsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerProServeToolsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 marzo 2026, 21:57 UTC
- Ora modificata: 23 marzo 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowProServeToolsFullAccess",
      "Effect" : "Allow",
      "Action" : "partnercentral-account-management:AccessProServeTools",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "partnercentral-account-management:ProServeRole" : [
            "AssessmentIndividualContributor",
            "AssessmentOrganizationReader",
            "AssessmentOrganizationContributor",
            "OrganizationAdmin"
          ]
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerProServeToolsIndividualContributor

Descrizione: fornisce l'accesso per creare e gestire le proprie valutazioni tramite ProServe strumenti.

`AWSPartnerProServeToolsIndividualContributor`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerProServeToolsIndividualContributor` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 marzo 2026, 21:57 UTC
- Ora modificata: 23 marzo 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsIndividualContributor`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowProServeToolsIndividualContributorAccess",
      "Effect" : "Allow",
      "Action" : "partnercentral-account-management:AccessProServeTools",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "partnercentral-account-management:ProServeRole" : [
            "AssessmentIndividualContributor"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPartnerProServeToolsOrganizationReaderIndividualContributor

Descrizione: fornisce l'accesso in lettura alle valutazioni organizzative con la possibilità di gestire le proprie valutazioni.

`AWSPartnerProServeToolsOrganizationReaderIndividualContributor`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPartnerProServeToolsOrganizationReaderIndividualContributor` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 marzo 2026, 22:12 UTC
- Ora modificata: 23 marzo 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsOrganizationReaderIndividualContributor`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowProServeToolsOrgReaderIndividualContributorAccess",
      "Effect" : "Allow",
      "Action" : "partnercentral-account-management:AccessProServeTools",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "partnercentral-account-management:ProServeRole" : [
            "AssessmentOrganizationReader",
            "AssessmentIndividualContributor"
          ]
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPCSComputeNodePolicy

Descrizione: concede l'autorizzazione ai nodi di calcolo AWS PCS per connettersi ai cluster AWS PCS.

`AWSPCSComputeNodePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSPCSComputeNodePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 giugno 2025, 18:07 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPCSComputeNodePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pcs:RegisterComputeNodeGroupInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPCSServiceRolePolicy

Descrizione: concede ai PCS le autorizzazioni per gestire le risorse per tuo conto.

`AWSPCSServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 27 agosto 2024, 16:01 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPCSServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsToCreatePCSNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToCreatePCSNetworkInterfacesInSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PermissionsToManagePCSNetworkInterfaces",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToDescribePCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreatePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "PermissionsToManagePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTerminatePCSManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*/AWSPCS*",
        "arn:aws:iam::*:role/AWSPCS*",
        "arn:aws:iam::*:role/aws-pcs/*",
        "arn:aws:iam::*:role/*/aws-pcs/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToControlClusterInstanceAttributes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:resource-groups:*:*:group/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Sid" : "PermissionsToProvisionClusterInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "PermissionsToTagPCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "CreateFleet",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToPublishMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/PCS"
        }
      }
    },
    {
      "Sid" : "PermissionsToManageSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:pcs!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "pcs",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPriceListServiceFullAccess

Descrizione: fornisce l'accesso completo al servizio di AWS listino prezzi.

`AWSPriceListServiceFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPriceListServiceFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 novembre 2017, 00:36 UTC
- Ora modificata: 02 luglio 2024, 13:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSPriceListServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricing:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPrivateCAAuditor

Descrizione: fornisce ai revisori l'accesso all'autorità di certificazione AWS privata

`AWSPrivateCAAuditor`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPrivateCAAuditor` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 febbraio 2023, 18:33 UTC
- Ora modificata: 14 febbraio 2023, 18:33 UTC

- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPrivateCAConnectorForKubernetesPolicy

Descrizione: concede le autorizzazioni essenziali per il AWS Private CA Connector for Kubernetes.

`AWSPrivateCAConnectorForKubernetesPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSPrivateCAConnectorForKubernetesPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 maggio 2025, 19:22 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAConnectorForKubernetesPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPrivateCAFullAccess

Descrizione: fornisce l'accesso completo all'autorità di certificazione AWS privata

`AWSPrivateCAFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPrivateCAFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 febbraio 2023, 18:20 UTC
- Ora modificata: 14 febbraio 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPrivateCAPrivilegedUser

Descrizione: fornisce agli utenti del certificato l'accesso privilegiato all'autorità di certificazione AWS privata

`AWSPrivateCAPrivilegedUser`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPrivateCAPrivilegedUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 febbraio 2023, 18:26 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
```

```
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPrivateCAReadOnly

Descrizione: fornisce l'accesso in sola lettura all'autorità di certificazione AWS privata

`AWSPrivateCAReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPrivateCAReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 febbraio 2023, 18:30 UTC
- Ora modificata: 14 febbraio 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPrivateCAUser

Descrizione: fornisce agli utenti del certificato l'accesso all'autorità di certificazione AWS privata

`AWSPrivateCAUser`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPrivateCAUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 febbraio 2023, 18:16 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:IssueCertificate"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
    "Condition" : {
      "ArnLike" : {
        "acm-pca:TemplateArn" : [
          "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
        ]
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "acm-pca:IssueCertificate"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
    "Condition" : {
      "ArnNotLike" : {
        "acm-pca:TemplateArn" : [
          "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:RevokeCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:ListPermissions"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:ListCertificateAuthorities"
    ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPrivateMarketplaceAdminFullAccess

Descrizione: fornisce l'accesso completo a tutte le azioni amministrative per un Marketplace AWS privato.

`AWSPrivateMarketplaceAdminFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPrivateMarketplaceAdminFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 16:32 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceGetRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*AWSServiceRoleForPrivateMarketplaceAdmin"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/private-
marketplace.marketplace.amazonaws.com/AWSServiceRoleForPrivateMarketplaceAdmin"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "private-marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceManageDelegatedAdministratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceEnableServiceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceRequestPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPrivateMarketplaceRequests

Descrizione: fornisce l'accesso alla creazione di richieste in un Marketplace AWS privato.

`AWSPrivateMarketplaceRequests`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSPrivateMarketplaceRequests` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 ottobre 2019, 21:44 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LegacyPrivateMarketplaceRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "PrivateMarketplaceManageRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateProductProcurementRequest",
            "CancelProductProcurementRequest"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceReadRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceListRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceReadChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
```

```
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceTaggingRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPrivateNetworksServiceRolePolicy

Descrizione: consente a AWS Private Networks Service di gestire le risorse per conto del cliente.

`AWSPrivateNetworksServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 16 dicembre 2021, 23:17 UTC
- Ora modificata: 16 dicembre 2021, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSProtonCodeBuildProvisioningBasicAccess

Descrizione: le autorizzazioni CodeBuild devono eseguire una build per AWS CodeBuild Proton Provisioning.

`AWSProtonCodeBuildProvisioningBasicAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSProtonCodeBuildProvisioningBasicAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 novembre 2022, 21:04 UTC
- Ora modificata: 09 novembre 2022, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/AWSProton-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "proton:NotifyResourceDeploymentStatusChange",
      "Resource" : "arn:aws:proton:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSProtonCodeBuildProvisioningServiceRolePolicy

Descrizione: consente a AWS Proton di gestire l'approvvigionamento di risorse Proton utilizzando CodeBuild e altri AWS servizi per conto dell'utente.

`AWSProtonCodeBuildProvisioningServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 09 novembre 2022, 21:32 UTC
- Ora modificata: 17 maggio 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSProton-CodeBuild-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject",
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:RetryBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:BatchGetProjects"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/AWSProton*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "codebuild.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSProtonDeveloperAccess

Descrizione: fornisce l'accesso a AWS Proton APIs and Management Console, ma non consente l'amministrazione di modelli o ambienti Proton.

`AWSProtonDeveloperAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSProtonDeveloperAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 febbraio 2021, 19:02 UTC

- Ora modificata: 6 giugno 2024, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "codestar-connections:UseConnection",
        "proton:CancelServiceInstanceDeployment",
        "proton:CancelServicePipelineDeployment",
        "proton:CreateService",
        "proton:DeleteService",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
```

```
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
        "proton:UpdateServicePipeline",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
```

```
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSProtonFullAccess

Descrizione: Fornisce l'accesso completo a AWS Proton APIs and Management Console. Oltre a queste autorizzazioni, è necessario anche l'accesso ad Amazon S3 per registrare pacchetti di modelli dai bucket S3, nonché l'accesso ad Amazon IAM per creare e gestire i ruoli di servizio per Proton.

`AWSProtonFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSProtonFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 febbraio 2021, 19:07 UTC
- Ora modificata: 6 giugno 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "proton.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/
AWSServiceRoleForProtonSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sync.proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:PassConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:PassConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSProtonReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS Proton APIs and Management Console.

`AWSProtonReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSProtonReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 febbraio 2021, 19:09 UTC
- Ora modificata: 18 novembre 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
```

```
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSProtonServiceGitSyncServiceRolePolicy

Descrizione: Politica che consente a AWS Proton di sincronizzare le definizioni del servizio, dell'ambiente e dei componenti dal repository git a Proton. AWS

`AWSProtonServiceGitSyncServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 4 aprile 2023, 15:55 UTC
- Ora modificata: 04 aprile 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonServiceSync",
      "Effect" : "Allow",
      "Action" : [
        "proton:GetService",
```

```
        "proton:UpdateService",
        "proton:UpdateServicePipeline",
        "proton:GetServiceInstance",
        "proton:CreateServiceInstance",
        "proton:UpdateServiceInstance",
        "proton:ListServiceInstances",
        "proton:GetComponent",
        "proton:CreateComponent",
        "proton:ListComponents",
        "proton:UpdateComponent",
        "proton:GetEnvironment",
        "proton:CreateEnvironment",
        "proton:ListEnvironments",
        "proton:UpdateEnvironment"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSProtonSyncServiceRolePolicy

Descrizione: Politica che consente a AWS Proton di sincronizzare i contenuti del tuo repository git con Proton o di sincronizzare i contenuti di Proton con i tuoi repository git.

`AWSProtonSyncServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 23 novembre 2021, 21:14 UTC
- Ora modificata: 5 maggio 2024, 01:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton:DeleteServiceTemplateVersion",
        "proton:DeleteEnvironmentTemplateVersion",
        "proton:CreateServiceTemplateVersion",
        "proton:CreateServiceTemplate",
        "proton:CreateEnvironmentTemplateVersion",
        "proton:CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton:CreateEnvironmentTemplateMajorVersion",
        "proton:CreateServiceTemplateMajorVersion"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSPurchaseOrdersServiceRolePolicy

Descrizione: concede le autorizzazioni per visualizzare e modificare gli ordini di acquisto sulla console di fatturazione

`AWSPurchaseOrdersServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSPurchaseOrdersServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 maggio 2020, 18:15 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "aws-portal:*Billing",
        "consolidatedbilling:GetAccountBillingRole",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceUnits",
        "payments:GetPaymentInstrument",
        "payments:ListPaymentPreferences",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupCFGCPacksPermissionsBoundary

Descrizione: la CFGCPacks PermissionsBoundary policy di AWSQuick installazione definisce l'elenco delle autorizzazioni consentite in un ruolo IAM creato da Quick Setup. Quick Setup utilizza un ruolo creato con questo criterio per distribuire i pacchetti di AWS conformità Config.

`AWSQuickSetupCFGCPacksPermissionsBoundary`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupCFGCPacksPermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 giugno 2024, 09:52 UTC
- Ora modificata: 26 giugno 2024, 09:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ]
    },
    {
      "Sid" : "ConfigurationRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutCPackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack"
      ],
      "Resource" : [
        "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeCPacksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConformancePacksSLRCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerSLRCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "EnableExplorerReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceSettingsForExplorerUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupDeploymentRolePolicy

Descrizione: fornisce le autorizzazioni per AWS Systems Manager Quick Setup per distribuire più tipi di configurazione. Questi tipi di configurazione creano ruoli e automazioni IAM che configurano i servizi e le funzionalità di Amazon Web Services utilizzati di frequente con le best practice consigliate.

`AWSQuickSetupDeploymentRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupDeploymentRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 giugno 2024, 09:55 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDeploymentRolePolicy`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CPacksRead",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePacks",
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "OpsPacksManage",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPackInstance-*"
      ]
    },
    {
      "Sid" : "QSDocsRead",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState"
      ]
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
```

```
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "EventRulesManage",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*QuickSetup-*"
      ]
    },
    {
      "Sid" : "CPacksSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "QSConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
```

```
      ]
    },
    {
      "Sid" : "QSConfigRolePass",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "QSConfigRoleBounded",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : [
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGRecordingPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRoleManagedPolicies",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSSystemsManagerEnableConfigRecordingExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy",
            "arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy",
            "arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupDevOpsGuruPermissionsBoundary

Descrizione: la AWSQuick SetupDevOpsGuruPermissionsBoundary policy definisce l'elenco delle autorizzazioni consentite in un ruolo IAM creato da Quick Setup. Quick Setup utilizza un ruolo creato con questa politica per abilitare e configurare Amazon DevOps Guru. Questa politica fornisce anche le autorizzazioni per abilitare Systems Manager Explorer.

`AWSQuickSetupDevOpsGuruPermissionsBoundary`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupDevOpsGuruPermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 giugno 2024, 09:44 UTC
- Ora modificata: 26 giugno 2024, 09:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateDevOpsGuruSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudformationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruNotificationChannelPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "devops-guru:AddNotificationChannel"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:DevOpsGuru-Default-Topic",
        "arn:aws:devops-guru:*:*:/channels"
      ]
    },
    {
      "Sid" : "DevOpsGuruConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:UpdateResourceCollection",
        "devops-guru:UpdateServiceIntegration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruDefaultSNSTopicConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:RemovePermission"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOpsGuru-Default-Topic"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
```

```
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupDistributorPermissionsBoundary

Descrizione: QuickSetup crea ruoli IAM che gli consentono di configurare la funzionalità Systems Manager Distributor per conto dell'utente e utilizza questa policy durante la creazione di tali ruoli per definire i limiti delle loro autorizzazioni.

`AWSQuickSetupDistributorPermissionsBoundary`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupDistributorPermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 giugno 2024, 09:50 UTC
- Ora modificata: 26 giugno 2024, 09:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DistributorAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ]
    },
    {
      "Sid" : "DistributorAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
```

```
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-ConfigureAWSPackage*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupEnableAREXExecutionPolicy

Descrizione: questo criterio concede le autorizzazioni che consentono a Systems Manager di eseguire il runbook di AWSQuickSetupType-EnableAREX automazione, che consente l'utilizzo di AWS Resource Explorer con Systems Manager.

`AWSQuickSetupEnableAREXExecutionPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupEnableAREXExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2024, 22:45 UTC
- Ora modificata: 15 novembre 2024, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableAREXExecutionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadActions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowUpdateExistingIndexAndAssociateDefaultView",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:AssociateDefaultView"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateViewAndIndex",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:TagResource"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*:*:view/all-resources/*",
        "arn:aws:resource-explorer-2:*:*:index/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/Type" : "QuickSetup",
          "aws:ResourceTag/Type" : "QuickSetup"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Type"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupEnableDHMCExecutionPolicy

Descrizione: questa policy concede le autorizzazioni che consentono ai principali di eseguire l' AWSQuickSetupType-EnableDHMC Automation Runbook, che abilita la configurazione predefinita della gestione dell'host.

`AWSQuickSetupEnableDHMCExecutionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupEnableDHMCExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2024, 21:27 UTC
- Ora modificata: 15 novembre 2024, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableDHMCExecutionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AmazonSSMManagedEC2InstanceDefaultPolicy"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/default-ec2-
instance-management-role"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupJITNADeploymentRolePolicy

Descrizione: questo criterio consente a Quick Setup di implementare il tipo di configurazione richiesto per configurare l'accesso ai just-in-time nodi.

`AWSQuickSetupJITNADeploymentRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupJITNADeploymentRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 aprile 2025, 09:07 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupJITNADeploymentRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-JITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
        "arn:aws:ssm:*::document/AWSQuickSetupType-
PropagateJustInTimeNodeAccessPolicies",
        "arn:aws:ssm:*:*:association/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "cloudformation.amazonaws.com"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::*:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-JITNA"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupManagedInstanceProfileExecutionPolicy

Descrizione: questa policy concede autorizzazioni amministrative che consentono a Systems Manager di creare un profilo di istanza IAM predefinito per la funzionalità Quick Setup e collegarlo a istanze Amazon EC2 che non dispongono già di un'istanza. profilo allegato.

`AWSQuickSetupManagedInstanceProfileExecutionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupManagedInstanceProfileExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2024, 21:51 UTC
- Ora modificata: 03 giugno 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManagedInstanceProfileExecutionPolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfilesForRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
```

```
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2AndSSMPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachAmazonSSMManagedInstanceCore",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess",
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
```

```
            "arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "InstanceProfileAssociationEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMInstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:UpdateManagedInstanceRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagRoles",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigId-*"
        }
      }
    },
    {
      "Sid" : "DenyModifyQuickSetupAutomationRoles",
      "Effect" : "Deny",
      "Action" : [
        "iam:TagRole",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
    },
```

```
    {
      "Sid" : "AutomationsStartWithTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ],
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AutomationsGetPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:GetAutomationExecution",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "GetQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
    },
    {
      "Sid" : "PassQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupManageJITNAResourcesExecutionPolicy

Descrizione: questo criterio fornisce le autorizzazioni per abilitare l'accesso ai just-in-time nodi per Systems Manager.

`AWSQuickSetupManageJITNAResourcesExecutionPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupManageJITNAResourcesExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 aprile 2025, 21:37 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateJustInTimeAccessServiceLinkedRole",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/justintimeaccess.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerJustInTimeAccess"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "justintimeaccess.ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateSystemsManagerNotificationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/notifications.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerNotifications"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "notifications.ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::*:policy/
AWSSystemsManagerJustInTimeAccessTokenPolicy"
        }
      }
    },
    {
```

```
      "Sid" : "IAMRoleManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      }
    },
    {
      "Sid" : "ServiceSettingsManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/just-in-time-access/identity-provider"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupPatchPolicyBaselineAccess

Descrizione: fornisce autorizzazioni di sola lettura per accedere alle linee di base delle patch configurate da un amministratore dell'organizzazione corrente Account AWS o dell'organizzazione tramite Quick Setup.

`AWSQuickSetupPatchPolicyBaselineAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupPatchPolicyBaselineAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 giugno 2024, 09:38 UTC
- Ora modificata: 26 giugno 2024, 09:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3SameAccountReadOnlyAccess",
```

```
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3OrganizationReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalOrgID" : [
            "${aws:ResourceOrgID}"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupPatchPolicyDeploymentRolePolicy

Descrizione: fornisce le autorizzazioni che consentono a Quick Setup di creare risorse associate a una configurazione di policy di patch.

`AWSQuickSetupPatchPolicyDeploymentRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupPatchPolicyDeploymentRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 giugno 2024, 09:57 UTC
- Ora modificata: 26 giugno 2024, 09:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyDeploymentRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3BucketsList",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AccessLogsBucketManage",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:Put*",
```

```
        "s3:Get*",
        "s3:List*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:s3:::aws-quicksetup-patchpolicy-access-log-*"
      ]
    },
    {
      "Sid" : "LambdaManage",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:UpdateFunction*",
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:DeleteFunction",
        "lambda:InvokeFunction",
        "lambda:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
```

```
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ]
    },
    {
      "Sid" : "LogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogGroupsManage",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource",
        "logs:PutRetentionPolicy",
        "logs:DeleteLogGroup",
        "logs:ListTagsForResource",
        "logs:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:DescribeDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
```

```
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*"
      ]
    },
    {
      "Sid" : "QSDocsGet",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline"
      ]
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "ConfigRolePassToSSM",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConfigRolePassToLambda",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "ConfigRoleBoundedManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AWSQuickSetupPatchPolicyPermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupPatchPolicyLambdaExecutionPolicy

Descrizione: concede le autorizzazioni per gestire le associazioni di State Manager per le operazioni di pulizia automatizzate quando le configurazioni di Quick Setup vengono eliminate.

`AWSQuickSetupPatchPolicyLambdaExecutionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupPatchPolicyLambdaExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 3 giugno 2026, 14:12 UTC
- Ora modificata: 03 giugno 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyLambdaExecutionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageSSMAssociations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:UpdateAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*"
      ]
    },
    {
      "Sid" : "PassQuickSetupAutomationRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupPatchPolicyPermissionsBoundary

Descrizione: QuickSetup crea ruoli IAM che gli consentono di configurare la funzionalità Systems Manager Patch Manager per conto dell'utente e utilizza questa politica durante la creazione di tali ruoli per definire i limiti delle loro autorizzazioni.

`AWSQuickSetupPatchPolicyPermissionsBoundary`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupPatchPolicyPermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 giugno 2024, 09:46 UTC
- Ora modificata: 5 marzo 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyPermissionsBoundary`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PatchingAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ]
    },
    {
      "Sid" : "PatchingAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
```

```
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess"
```

```
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManagedInstanceRoleUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateManagedInstanceRole"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "InstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "InstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "InstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:UpdateAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "BaselineS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:Put*",
        "s3:Get*",
        "s3:List*",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteBucket"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
```

```
      },
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*"
    },
    {
      "Sid" : "PatchingFunctionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "LoggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "SSMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
```

```
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "EC2TaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "RoleTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigId-*"
        }
      }
    },
    {
      "Sid" : "PatchingReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetPatchBaseline",
        "ssm:GetInventory",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAssociation",
        "ssm:GetAutomationExecution",
        "ssm:ListTagsForResource",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PatchingAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/QuickSetup-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:document/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupPatchPolicyTagManagementExecutionPolicy

Descrizione: concede le autorizzazioni per tenere traccia delle istanze gestite dalle configurazioni delle policy di patch di Quick Setup tramite l'etichettatura automatica e la raccolta dell'inventario.

`AWSQuickSetupPatchPolicyTagManagementExecutionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupPatchPolicyTagManagementExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 giugno 2026, 14:12 UTC
- Ora modificata: 03 giugno 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyTagManagementExecutionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GetSSMInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageSSMManagedInstanceTags",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "ManageEC2InstanceTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
```

```
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupSchedulerPermissionsBoundary

Descrizione: la AWSQuickSetupSchedulerPermissionsBoundary policy definisce l'elenco delle autorizzazioni consentite in un ruolo IAM creato da Quick Setup. Quick Setup utilizza un ruolo creato con questa policy per abilitare e configurare operazioni pianificate su istanze Amazon EC2 e altre risorse.

`AWSQuickSetupSchedulerPermissionsBoundary`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupSchedulerPermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 26 giugno 2024, 09:53 UTC
- Ora modificata: 26 giugno 2024, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ]
    },
    {
      "Sid" : "ConfigurationAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "SystemsManagerCalendarReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar-*"
      ]
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2StartStopPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AutomationStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
StartStateManagerAssociations-*"
      ]
    },
    {
      "Sid" : "AssociationsStartOncePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupSSMDeploymentRolePolicy

Descrizione: questa politica concede autorizzazioni amministrative che consentono a Quick Setup di creare risorse da utilizzare durante il processo di onboarding di Systems Manager.

`AWSQuickSetupSSMDeploymentRolePolicy`AWS è una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupSSMDeploymentRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2024, 22:53 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
```

```
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-SSM-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunction*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
```

```
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/
AWSQuickSetupSSMLifecycleManagementExecutionPolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupSSMManageResourcesExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
ExecutionRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
OperationalAccountAdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
            "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
            "arn:aws:ssm:*::document/AWS-EnableExplorer",
            "arn:aws:ssm:*:*:association/*"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : "arn:aws:ssm:*::document/AWSQuickSetupType-SSM-ManageResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeAssociationExecutionTargets",
        "ssm:GetAutomationExecution"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupSSMDeploymentS3BucketRolePolicy

Descrizione: questa politica concede le autorizzazioni per elencare tutti i bucket S3 in un account e per gestire e recuperare informazioni su bucket specifici nell'account principale gestiti tramite modelli. AWS CloudFormation

`AWSQuickSetupSSMDeploymentS3BucketRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupSSMDeploymentS3BucketRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2024, 22:01 UTC
- Ora modificata: 15 novembre 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentS3BucketRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketTagging",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupSSMHostMgmtPermissionsBoundary

Descrizione: Quick Setup crea ruoli IAM che gli consentono di configurare il tipo di configurazione rapida di Host Manager per conto dell'utente e utilizza questa politica durante la creazione di tali ruoli per definire i limiti delle relative autorizzazioni.

`AWSQuickSetupSSMHostMgmtPermissionsBoundary`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupSSMHostMgmtPermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 giugno 2024, 09:48 UTC
- Ora modificata: 26 giugno 2024, 09:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HostManagementAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ]
    },
    {
      "Sid" : "HostManagementAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation"
          ]
```

```
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
```

```
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-HostMgmt-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
CreateAndAttachIAMToInstance-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
UpdateExistingInstanceProfile-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
InstallAndManageCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/AWSEC2-UpdateLaunchAgent-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-GatherSoftwareInventory*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaselineAssociation*",
        "arn:aws:ssm:*:*:automation-definition/AWS-UpdateSSMAgent*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupSSMLifecycleManagementExecutionPolicy

Descrizione: la politica concede autorizzazioni amministrative che consentono a Quick Setup di eseguire una risorsa AWS CloudFormation personalizzata sugli eventi del ciclo di vita durante la distribuzione di Quick Setup in Systems Manager.

`AWSQuickSetupSSMLifecycleManagementExecutionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupSSMLifecycleManagementExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2024, 21:55 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMLifecycleManagementExecutionPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupSSMManageResourcesExecutionPolicy

Descrizione: questa policy concede autorizzazioni che consentono a Systems Manager di creare prerequisiti come i ruoli IAM richiesti per l'onboarding di Systems Manager.

`AWSQuickSetupSSMManageResourcesExecutionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupSSMManageResourcesExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2024, 22:49 UTC
- Ora modificata: 15 novembre 2024, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMManageResourcesExecutionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableDHMCExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableAREXExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:DeleteObject",
        "s3:ListBucketVersions",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupStartSSMAssociationsExecutionPolicy

Descrizione: questa politica concede le autorizzazioni che consentono ai responsabili di eseguire il runbook di AWSQuickSetupType-StartSSMAssociations automazione, che avvia State Manager Associations.

`AWSQuickSetupStartSSMAssociationsExecutionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupStartSSMAssociationsExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 agosto 2025, 12:04 UTC
- Ora modificata: 5 marzo 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
            "arn:aws:ssm:*:*:automation-execution/*",
            "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSetupStartStopInstancesExecutionPolicy

Descrizione: la policy gestita AWSQuickSetupStartStopInstancesExecutionPolicy fornisce le autorizzazioni per Quick Setup per avviare e arrestare le istanze Amazon EC2 secondo una pianificazione. Questa politica viene utilizzata con il tipo di configurazione dello scheduler Quick Setup.

`AWSQuickSetupStartStopInstancesExecutionPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSetupStartStopInstancesExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 agosto 2025, 12:04 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ApplyInstanceState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightAssetBundleExportPolicy

Descrizione: fornisce il set di autorizzazioni necessarie per eseguire le operazioni di esportazione di QuickSight Asset Bundle

`AWSQuickSightAssetBundleExportPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightAssetBundleExportPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 marzo 2024, 21:31 UTC
- Ora modificata: 27 marzo 2024, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:ListRefreshSchedules",
        "quicksight:DescribeDataSetPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
      "Sid" : "DataSourceReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
```

```
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "VPCConnectionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeVPCConnection",
        "quicksight:ListVPCConnections"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "RefreshScheduleReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "AssetBundleExportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleExportJob",
        "quicksight:ListAssetBundleExportJobs",
        "quicksight:StartAssetBundleExportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-export-job/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightAssetBundleImportPolicy

Descrizione: fornisce il set di autorizzazioni necessarie per eseguire le operazioni di importazione di QuickSight Asset Bundle

`AWSQuickSightAssetBundleImportPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightAssetBundleImportPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 marzo 2024, 21:40 UTC
- Ora modificata: 27 marzo 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource",
        "quicksight:TagResource",
        "quicksight:UntagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDashboard",
        "quicksight:DeleteDashboard",
        "quicksight:DescribeDashboard",
        "quicksight:UpdateDashboard",
        "quicksight:UpdateDashboardPublishedVersion",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:UpdateDashboardPermissions",
        "quicksight:UpdateDashboardLinks"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateAnalysis",
        "quicksight:DeleteAnalysis",
        "quicksight:DescribeAnalysis",
        "quicksight:UpdateAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:UpdateAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetWriteAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "quicksight:CreateDataSet",
        "quicksight:DeleteDataSet",
        "quicksight:DescribeDataSet",
        "quicksight:PassDataSet",
        "quicksight:UpdateDataSet",
        "quicksight:DeleteDataSetRefreshProperties",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:PutDataSetRefreshProperties",
        "quicksight:UpdateDataSetPermissions",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:ListRefreshSchedules"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
      "Sid" : "DataSourceWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:DescribeDataSource",
        "quicksight:DeleteDataSource",
        "quicksight:PassDataSource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateTheme",
        "quicksight:DeleteTheme",
        "quicksight:DescribeTheme",
        "quicksight:UpdateTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:UpdateThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "RefreshScheduleWriteAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "quicksight:CreateRefreshSchedule",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DeleteRefreshSchedule",
        "quicksight:UpdateRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "VPCConnectionWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListVPCConnections",
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "AssetBundleImportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleImportJob",
        "quicksight:ListAssetBundleImportJobs",
        "quicksight:StartAssetBundleImportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuicksightAthenaAccess

Descrizione: accesso Quicksight all'API Athena e ai bucket S3 utilizzati per i risultati delle query Athena

`AWSQuicksightAthenaAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSQuicksightAthenaAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 09 dicembre 2016, 02:31 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
```

```
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",
        "athena:ListQueryExecutions",
        "athena:RunQuery",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:ListWorkGroups",
        "athena:ListEngineVersions",
        "athena:GetWorkGroup",
        "athena:GetDataCatalog",
        "athena:GetDatabase",
        "athena:GetTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
```

```
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightDescribeRDS

Descrizione: consente di QuickSight descrivere le risorse RDS

`AWSQuickSightDescribeRDS`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightDescribeRDS` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 novembre 2015, 23:24 UTC
- Ora modificata: 10 novembre 2015, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:Describe*"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightDescribeRedshift

Descrizione: consente di QuickSight descrivere le risorse Redshift

`AWSQuickSightDescribeRedshift`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightDescribeRedshift` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 novembre 2015, 23:25 UTC
- Ora modificata: 10 novembre 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightElasticsearchPolicy

Descrizione: Fornisce accesso alle risorse Amazon Elasticsearch di Amazon QuickSight

`AWSQuickSightElasticsearchPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightElasticsearchPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 09 settembre 2020, 17:27 UTC
- Ora modificata: 07 settembre 2021, 23:25 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeElasticsearchDomain",
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightIoTAnalyticsAccess

Descrizione: Offri l'accesso in QuickSight sola lettura ai set di dati di IoT Analytics

`AWSQuickSightIoTAnalyticsAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightIoTAnalyticsAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 17:00 UTC
- Ora modificata: 29 novembre 2017, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iotanalytics:ListDatasets",
        "iotanalytics:DescribeDataset",
        "iotanalytics:GetDatasetContent"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightListIAM

Descrizione: consente di QuickSight elencare le entità IAM

`AWSQuickSightListIAM`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightListIAM` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 10 novembre 2015, 23:25 UTC
- Ora modificata: 10 novembre 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuicksightOpenSearchPolicy

Descrizione: Fornisce l'accesso alle OpenSearch risorse Amazon da Amazon QuickSight

`AWSQuicksightOpenSearchPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuicksightOpenSearchPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 07 settembre 2021, 23:26 UTC
- Ora modificata: 07 settembre 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightSageMakerPolicy

Descrizione: Fornisce l'accesso alle SageMaker risorse Amazon da Amazon QuickSight

`AWSQuickSightSageMakerPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightSageMakerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 17 gennaio 2020, 17:18 UTC
- Ora modificata: 30 ottobre 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
```

```
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListModels",
        "sagemaker:DescribeModel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::quicksight-ml.*",
        "arn:aws:s3:::sagemaker*"
      ]
    },
    {
      "Sid" : "S3ObjectUpdateAccess",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::sagemaker*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3BucketReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::sagemaker*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightSecretsManagerWriteAccess

Descrizione: Politica utilizzata QuickSight per creare AWS segreti in Secrets Manager e per allegare politiche di risorse ai QuickSight segreti esistenti.

`AWSQuickSightSecretsManagerWriteAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightSecretsManagerWriteAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 22 maggio 2025, 01:22 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSecretsManagerWriteAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightSecretsManagerWritePolicy

Descrizione: Politica utilizzata QuickSight per creare AWS segreti in Secrets Manager e per allegare politiche di risorse ai QuickSight segreti esistenti.

`AWSQuickSightSecretsManagerWritePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightSecretsManagerWritePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 maggio 2025, 19:22 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightSecretsManagerWritePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSQuickSightTimestreamPolicy

Descrizione: AWS QuickSight accesso a AWS Timestream APIs. I clienti possono associare questa politica al AWS QuickSight ruolo per consentire il recupero di dati e metadati.

`AWSQuickSightTimestreamPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSQuickSightTimestreamPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 30 settembre 2020, 21:47 UTC

- Ora modificata: 30 settembre 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:Select",
        "timestream:CancelQuery",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase",
        "timestream:SelectValues",
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSReachabilityAnalyzerServiceRolePolicy

Descrizione: consente a VPC Reachability Analyzer di accedere alle AWS risorse e integrarsi con AWS Organizations per tuo conto.

`AWSReachabilityAnalyzerServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 23 novembre 2022, 17:12 UTC
- Ora modificata: 10 settembre 2024, 16:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReachabilityAnalyzerPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
```

```
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "tag:GetResources",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApigatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRefactoringToolkitFullAccess

Descrizione: questo criterio concede l'autorizzazione a utilizzare i AWS servizi con l'estensione AWS Toolkit for .NET Refactoring per Microsoft Visual Studio. È destinato a essere collegato a un profilo locale. AWS La policy consente di caricare elementi dell'applicazione e scaricare gli artefatti risultanti da Amazon S3. Consente di creare applicazioni in un'immagine del contenitore utilizzando, archiviando AWS CodeBuild e recuperando le immagini da Amazon Elastic Container Registry (Amazon ECR). Inoltre, consente l'implementazione dell'applicazione su servizi container AWS come Amazon Elastic Container Service (Amazon ECS), la creazione opzionale di risorse VPC, la connessione opzionale all'infrastruttura esistente come Directory AWS Service e altri servizi correlati.

`AWSRefactoringToolkitFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSRefactoringToolkitFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 ottobre 2022, 16:41 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild"
      ],
```

```
      "Resource" : "arn:aws:codebuild:*:*:project/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupIngress",
            "CreateInternetGateway",
            "CreateKeyPair",
            "CreateRoute",
            "CreateRouteTable",
            "CreateSubnet",
            "CreateVpc"
          ]
        },
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
```

```
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "a2c-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "application-transformation-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
```

```
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "a2c-generated"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "application-transformation"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::*/refactoringtoolkit*",
        "arn:aws:s3:::*/a2c-generated*",
        "arn:aws:s3:::*/application-transformation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "application-transformation",
            "refactoringtoolkit"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "clouddirectory:ListDirectories",
        "codebuild:BatchGetProjects",
        "codebuild:BatchGetBuilds",
        "ds:DescribeDirectories",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ecr:DescribeImages",
        "ecr:DescribeRepositories",
        "ecs:DescribeClusters",
```

```
        "ecs:DescribeServices",
        "ecs:DescribeTasks",
        "ecs:ListTagsForResource",
        "ecs:ListTasks",
        "iam:ListRoles",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment",
        "application-transformation:PutLogData",
        "application-transformation:PutMetricData",
        "application-transformation:StartContainerization",
        "application-transformation:GetContainerization",
        "application-transformation:StartDeployment",
        "application-transformation:GetDeployment"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "ecr:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
```

```
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRefactoringToolkitSidecarPolicy

Descrizione: questa policy è pensata per essere utilizzata da Amazon ECS Tasks creati per testare le applicazioni AWS utilizzando l'estensione AWS Toolkit for .NET Refactoring per Microsoft Visual Studio. La policy consente l'accesso per scaricare artefatti applicativi da Amazon S3, comunicare lo stato del Task tramite AWS Systems Manager e altri servizi richiesti.

`AWSRefactoringToolkitSidecarPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSRefactoringToolkitSidecarPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 ottobre 2022, 16:41 UTC
- Ora modificata: 29 ottobre 2022, 22:15 UTC

- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenControlChannel",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssmmessages:CreateDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/refactoringtoolkit*"
    },
    {
      "Sid" : "S3ListBucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
```

```
        "StringLike" : {
          "s3:prefix" : "refactoringtoolkit*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSrePostPrivateCloudWatchAccess

Descrizione: fornisce a Re:POST l'accesso privato per pubblicare CloudWatch i dati delle metriche

`AWSrePostPrivateCloudWatchAccess`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 novembre 2023, 16:37 UTC
- Ora modificata: 15 novembre 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPublishMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/rePostPrivate",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRepostSpaceSupportOperationsPolicy

Descrizione: questa politica consente al servizio re:Post Space di creare, gestire e risolvere i casi di supporto creati tramite l'applicazione Space.

`AWSRepostSpaceSupportOperationsPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSRepostSpaceSupportOperationsPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 novembre 2023, 21:52 UTC
- Ora modificata: 26 novembre 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResilienceHubAsssessmentExecutionPolicy

Descrizione: Policy per il ruolo del servizio AWS Resilience Hub che consente l'accesso ad altri AWS servizi per eseguire la valutazione.

`AWSResilienceHubAsssessmentExecutionPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSResilienceHubAsssessmentExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2023, 12:32 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "docdb-elastic:GetCluster",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListTagsForResource",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
```

```
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ecr:DescribeRegistry",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeServerlessCacheSnapshots",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperiment",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListExperimentResolvedTargets",
```

```
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "rds:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:ListBucket",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3ArtifactStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubS3AccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "ResilienceHub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubSSMStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResilienceHubResilienceTestingPolicy

Descrizione: ruolo del servizio Policy for AWS Resilience Hub che consente l'accesso al servizio AWS Fault Injection per avviare i test di resilienza.

`AWSResilienceHubResilienceTestingPolicy`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSResilienceHubResilienceTestingPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 31 luglio 2026, 22:27 UTC
- Ora modificata: 31 luglio 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubResilienceTestingPolicy`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFISActionStatement",
      "Effect" : "Allow",
      "Action" : "fis:CreateExperimentTemplate",
      "Resource" : "arn:aws:fis:*:*:action/*"
    },
    {
      "Sid" : "AWSResilienceHubFISCreateExperimentTemplateStatement",
```

```
      "Effect" : "Allow",
      "Action" : "fis:CreateExperimentTemplate",
      "Resource" : "arn:aws:fis:*:*:experiment-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISStartExperimentFromTemplateStatement",
      "Effect" : "Allow",
      "Action" : "fis:StartExperiment",
      "Resource" : "arn:aws:fis:*:*:experiment-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISStartExperimentStatement",
      "Effect" : "Allow",
      "Action" : "fis:StartExperiment",
      "Resource" : "arn:aws:fis:*:*:experiment/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISExperimentStatement",
      "Effect" : "Allow",
      "Action" : [
        "fis:GetExperiment",
        "fis:StopExperiment",
        "fis:ListExperimentResolvedTargets"
      ],
      "Resource" : "arn:aws:fis:*:*:experiment/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/managedBy" : "resiliencehub"
        }
```

```
      }
    },
    {
      "Sid" : "AWSResilienceHubFISExperimentTemplateStatement",
      "Effect" : "Allow",
      "Action" : [
        "fis:CreateTargetAccountConfiguration",
        "fis:DeleteExperimentTemplate"
      ],
      "Resource" : "arn:aws:fis:*:*:experiment-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISTagResourceStatement",
      "Effect" : "Allow",
      "Action" : "fis:TagResource",
      "Resource" : [
        "arn:aws:fis:*:*:experiment-template/*",
        "arn:aws:fis:*:*:experiment/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubRegionSwitchStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:GetPlanExecution"
      ],
      "Resource" : "arn:aws:arc-region-switch::*:plan/*:*"
    },
    {
      "Sid" : "AWSResilienceHubFISCreateSLRStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchAlarmStatement",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarmHistory",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResilienceHubServiceRolePolicy

Descrizione: consente a AWS Resilience Hub di accedere alle risorse del tuo account per l'individuazione, la valutazione e la gestione della resilienza.

`AWSResilienceHubServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 28 maggio 2026, 17:42 UTC
- Ora modificata: 6 luglio 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResilienceHubServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubOrganizationsReadStatement",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListDelegatedServicesForAccount",
```

```
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "organizations:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResilienceHubV2AssessmentExecutionPolicy

Descrizione: consente a AWS Resilience Hub di accedere alle risorse del tuo account per l'individuazione, la valutazione e la gestione della resilienza. Questa politica concede autorizzazioni di sola lettura con caratteri predefiniti che possono includere informazioni sensibili nell'output.

`AWSResilienceHubV2AssessmentExecutionPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSResilienceHubV2AssessmentExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 giugno 2026, 22:57 UTC
- Ora modificata: 17 giugno 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubV2AssessmentExecutionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubV2ReadResourceConfigStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "application-autoscaling:Describe*",
        "application-autoscaling:GetPredictiveScalingForecast",
        "application-autoscaling:ListTagsForResource",
        "arc-region-switch:Get*",
        "arc-region-switch:List*",
        "arc-zonal-shift:Get*",
        "arc-zonal-shift:List*",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "config:Describe*",
```

```
        "config:GetStoredQuery",
        "config:List*",
        "datasync:Describe*",
        "datasync:List*",
        "dlm:Get*",
        "docdb-elastic:Get*",
        "docdb-elastic:List*",
        "drs:Describe*",
        "drs:Get*",
        "drs:List*",
        "ds:Describe*",
        "dsql:Get*",
        "dsql:List*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeClientVpnConnections",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ecr:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "events:Describe*",
        "events:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fis:Get*",
        "fis:List*",
        "fsx:Describe*",
        "fsx:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "iam:GetInstanceProfile",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
```

```
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListRoleTags",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kinesis:Describe*",
        "kinesis:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "qldb:Describe*",
        "qldb:List*",
        "ram:Get*",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift:Describe*",
        "redshift:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "route53-recovery-cluster:Get*",
```

```
        "route53-recovery-cluster:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:Get*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53domains:Check*",
        "route53domains:List*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListBucket",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm:Describe*",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:List*",
        "states:Describe*",
        "states:List*",
        "tag:GetResources",
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "wafv2:Get*",
```

```
        "wafv2:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3AccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResourceAccessManagerFullAccess

Descrizione: Fornisce l'accesso completo a AWS Resource Access Manager

`AWSResourceAccessManagerFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSResourceAccessManagerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 giugno 2019, 17:28 UTC
- Ora modificata: 04 giugno 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "ram:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResourceAccessManagerReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a AWS Resource Access Manager.

`AWSResourceAccessManagerReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSResourceAccessManagerReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 dicembre 2019, 20:58 UTC
- Ora modificata: 09 dicembre 2019, 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResourceAccessManagerResourceShareParticipantAccess

Descrizione: fornisce l'accesso al AWS Resource Access Manager APIs necessario a un partecipante alla condivisione delle risorse.

`AWSResourceAccessManagerResourceShareParticipantAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSResourceAccessManagerResourceShareParticipantAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 dicembre 2019, 20:41 UTC
- Ora modificata: 09 dicembre 2019, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",
        "ram:RejectResourceShareInvitation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResourceAccessManagerServiceRolePolicy

Descrizione: Policy che include l'accesso in modalità Read-only Read-Only AWS Resource Access Manager alla struttura Organizations dei clienti. Contiene anche le autorizzazioni IAM per eliminare autonomamente il ruolo.

`AWSResourceAccessManagerServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 novembre 2018, 19:28 UTC
- Ora modificata: 14 novembre 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResourceExplorerFullAccess

Descrizione: questa politica concede autorizzazioni amministrative per accedere alle risorse di Resource Explorer e concede autorizzazioni di sola lettura ad altri AWS servizi per supportare questo accesso.

`AWSResourceExplorerFullAccess`AWS è una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSResourceExplorerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 07 novembre 2022, 20:01 UTC
- Ora modificata: 14 novembre 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerConsoleFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
```

```
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResourceExplorerOrganizationsAccess

Descrizione: questa politica concede autorizzazioni amministrative a Resource Explorer e concede autorizzazioni di sola lettura ad altri AWS servizi per supportare questo accesso. L'amministratore di AWS Organizations necessita di queste autorizzazioni per configurare e gestire la ricerca su più account nella console.

`AWSResourceExplorerOrganizationsAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSResourceExplorerOrganizationsAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 novembre 2023, 17:01 UTC
- Ora modificata: 14 novembre 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerGetSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    },
    {
      "Sid" : "ResourceExplorerCreateSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationsAdministratorAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResourceExplorerReadOnlyAccess

Descrizione: questa politica concede autorizzazioni di sola lettura per cercare e visualizzare le risorse di Resource Explorer e concede autorizzazioni di sola lettura ad altri servizi per supportare questo accesso. AWS

`AWSResourceExplorerReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSResourceExplorerReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Tempo di creazione: 07 novembre 2022, 19:56 UTC
- Ora modificata: 14 novembre 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-explorer-2:BatchGetView",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResourceExplorerServiceRolePolicy

Descrizione: consente a Resource Explorer di visualizzare risorse ed CloudTrail eventi per conto dell'utente per indicizzare le risorse per la ricerca.

`AWSResourceExplorerServiceRolePolicy`è una policy AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 25 ottobre 2022, 20:35 UTC
- Ora modificata: 31 luglio 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Versione della politica

Versione della politica: v52 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerAndOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:DeleteIndex",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
```

```
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-
explorer-2/*"
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "access-analyzer:GetAnalyzer",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:ListCertificates",
        "airflow:ListEnvironments",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "aoss:ListCollections",
        "app-integrations:GetApplication",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:ListApplications",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
```

```
        "appstream:ListTagsForResource",
        "appsync:ListGraphqlApis",
        "aps:DescribeRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "auditmanager:ListTagsForResource",
        "autoscaling:DescribeAutoScalingGroups",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:ListSchedulingPolicies",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock:GetFlowAlias",
        "bedrock:GetInferenceProfile",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgents",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:ViewBudget",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
```

```
        "chime:ListAppInstanceBots",
        "chime:ListAppInstanceUsers",
        "chime:ListAppInstances",
        "chime:ListMediaInsightsPipelineConfigurations",
        "chime:ListMediaPipelineKinesisVideoStreamPools",
        "chime:ListMediaPipelines",
        "chime:ListSipMediaApplications",
        "chime:ListVoiceConnectors",
        "cleanrooms:GetCollaboration",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListTagsForResource",
        "cloud9:ListEnvironments",
        "cloudformation:ListResources",
        "cloudformation:ListStackSets",
        "cloudformation:ListStacks",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributions",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudhsm:DescribeClusters",
        "cloudtrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListRepositories",
```

```
        "codeartifact:ListTagsForResource",
        "codebuild:ListProjects",
        "codecommit:ListRepositories",
        "codeconnections:ListConnections",
        "codeconnections:ListHosts",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListTagsForResource",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:ListTagsForResource",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:ListTagsForResource",
        "codepipeline:ListPipelines",
        "codepipeline:ListWebhooks",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListDocumentClassifiers",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:DescribeConfigRules",
        "connect:DescribeInstance",
        "connect:DescribePhoneNumber",
        "connect:DescribeQuickConnect",
        "connect:DescribeRule",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListEvaluationForms",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListPhoneNumbersV2",
```

```
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityProfiles",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListDataSets",
        "datapipeline:ListPipelines",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "detective:ListGraphs",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTestGridProjects",
        "directconnect:DescribeDirectConnectGateways",
        "dlm:GetLifecyclePolicies",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTasks",
        "ds:DescribeDirectories",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
```

```
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayMulticastDomains",
```

```
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSubnetCidrReservations",
        "ecr-public:DescribeRepositories",
        "ecr:DescribeRepositories",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeServices",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeReservedCacheNodes",
```

```
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "emr-containers:ListJobTemplates",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListSecurityConfigurations",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:ListApplications",
        "es:ListDomainNames",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "finspace:ListEnvironments",
        "firehose:ListDeliveryStreams",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
```

```
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetVariables",
        "fsx:DescribeBackups",
        "fsx:DescribeFileSystems",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListTrackers",
        "glacier:ListVaults",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetJobs",
        "glue:GetTables",
        "glue:GetTriggers",
        "glue:ListDataQualityRulesets",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "grafana:ListWorkspaces",
        "greengrass:ListComponentVersions",
        "greengrass:ListComponents",
        "greengrass:ListConnectorDefinitions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListResourceDefinitions",
        "greengrass:ListSubscriptionDefinitions",
        "groundstation:ListConfigs",
```

```
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListThreatIntelSets",
        "healthlake:ListFHIRDatastores",
        "iam:ListGroups",
        "iam:ListInstanceProfiles",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:ListFilters",
        "inspector:ListAssessmentTemplates",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListJobs",
        "iot:ListMitigationActions",
        "iot:ListOTAUpdates",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
```

```
        "iot:ListSecurityProfiles",
        "iot:ListStreams",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListTunnels",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotfleethub:ListApplications",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListVehicles",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjects",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "iotwireless:ListWirelessGateways",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
```

```
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:ListClusters",
        "kafka:ListConfigurations",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra:ListAccessControlConfigurations",
        "kendra:ListDataSources",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListFeaturedResultsSets",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListThesauri",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kms:ListKeys",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayerVersions",
        "lambda:ListLayers",
        "lambda:ListVersionsByFunction",
        "lex:ListBotAliases",
        "lex:ListBots",
        "license-manager:ListDistributedGrants",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:ListTagsForResource",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:ListEnvironments",
```

```
        "macie2:ListAllowLists",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListMembers",
        "managedblockchain:ListAccessors",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediastore:ListContainers",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTemplates",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "oam:ListSinks",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListWorkflows",
        "organizations:DescribeResourcePolicy",
        "organizations:ListPolicies",
```

```
        "outposts:ListSites",
        "panorama:ListDevices",
        "panorama:ListPackages",
        "partnercentral:ListBenefitApplications",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "pipes:ListPipes",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceTemplates",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListLedgers",
        "quicksight:DescribeAccountSubscription",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetResourceShares",
        "ram:ListPermissions",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:DescribeBlueGreenDeployments",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
```

```
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeReservedDBInstances",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeHsmClientCertificates",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "rekognition:ListCollections",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListApps",
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53domains:ListDomains",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigs",
```

```
        "route53resolver:ListResolverRules",
        "rum:ListAppMonitors",
        "s3:GetBucketLocation",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3express:ListAllMyDirectoryBuckets",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListContexts",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
```

```
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:ListScheduleGroups",
        "schemas:ListDiscoverers",
        "secretsmanager:ListSecrets",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAttributeGroups",
        "servicediscovery:ListServices",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailIdentities",
        "ses:ListEmailTemplates",
        "shield:ListProtectionGroups",
        "shield:ListProtections",
        "signer:ListSigningProfiles",
        "sns:ListTopics",
        "sqs:ListQueues",
        "ssm-incidents:ListResponsePlans",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribeSessions",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListFileShares",
        "storagegateway:ListGateways",
        "swf:ListDomains",
        "synthetics:DescribeCanaries",
        "synthetics:ListGroups",
        "transfer:ListAgreements",
```

```
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "verifiedpermissions:ListPolicyStores",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "wafv2:ListIPSets",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListRuleGroups",
        "wafv2:ListWebACLs",
        "wellarchitected:ListWorkloads",
        "wisdom:ListAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:ListContents",
        "wisdom:ListKnowledgeBases",
        "workspaces-web:ListPortals",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaces",
        "xray:GetSamplingRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsForReadGetResources",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
        "backup:ListTags",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetFlowAlias",
```

```
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "cleanrooms:GetCollaboration",
        "cleanrooms:ListMembers",
        "cleanrooms:ListTagsForResource",
        "cloudformation:GetResource",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "connect:DescribeQueue",
        "connect:ListInstances",
        "connect:ListQuickConnects",
        "connect:ListUserProficiencies",
        "connect:ListUsers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "dataexchange:GetRevision",
        "dataexchange:ListTagsForResource",
        "datasync:DescribeTask",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "detective:DescribeOrganizationConfiguration",
        "detective:ListTagsForResource",
        "dlm:GetLifecyclePolicy",
        "dlm:ListTagsForResource",
```

```
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVolumeAttribute",
        "ecs:DescribeClusters",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTagsForResource",
        "eks:DescribeCluster",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:ListDomainsForPackage",
        "es:ListTags",
        "es:ListVpcEndpointsForDomain",
        "events:DescribeRule",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "fis:GetExperiment",
        "fis:GetExperimentTemplate",
        "fis:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
```

```
        "gamelift:DescribeScript",
        "gamelift:ListBuilds",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeAcceleratorAttributes",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListTagsForResource",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListTagsForResource",
        "greengrass:DescribeComponent",
        "greengrass:ListTagsForResource",
        "groundstation:GetConfig",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListTagsForResource",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "ivs:GetPlaybackKeyPair",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListTagsForResource",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListTagsForResource",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListTagsForResource",
        "kinesis:ListTagsForStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
```

```
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListTags",
        "logs:DescribeIndexPolicies",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "mediaconnect:DescribeFlow",
        "organizations:DescribeOrganization",
        "panorama:DescribeDevice",
        "panorama:ListTagsForResource",
        "partnercentral:GetBenefitApplication",
        "partnercentral:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "ram:GetPermission",
        "rds:ListTagsForResource",
        "redshift:DescribeTags",
        "resource-explorer-2:GetView",
        "route53:GetHostedZone",
        "route53:ListQueryLoggingConfigs",
        "route53:ListTagsForResource",
        "s3:GetAccelerateConfiguration",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketCORS",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
```

```
        "s3:GetReplicationConfiguration",
        "s3:ListTagsForResource",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "sagemaker:DescribeEndpoint",
        "sagemaker:ListTags",
        "schemas:DescribeDiscoverer",
        "schemas:ListDiscoverers",
        "secretsmanager:DescribeSecret",
        "sns:GetDataProtectionPolicy",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "vpc-lattice:GetAccessLogSubscription",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSResourceGroupsReadOnlyAccess

Descrizione: questa è la politica di sola lettura per AWS Resource Groups

`AWSResourceGroupsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSResourceGroupsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 marzo 2018, 10:27 UTC
- Ora modificata: 5 febbraio 2019, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "tag:Get*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeSnapshots",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListClusters",
        "glacier:ListVaults",
```

```
        "glacier:DescribeVault",
        "glacier:ListTagsForVault",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:ListTagsForStream",
        "opsworks:DescribeStacks",
        "opsworks:ListTags",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "route53domains:ListDomains",
        "route53:ListHealthChecks",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:GetHostedZone",
        "route53:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "ssm:ListDocuments"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRevenueAttributionManagement

Descrizione: fornisce l'accesso necessario per le attività di gestione dell'attribuzione dei ricavi.

`AWSRevenueAttributionManagement`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSRevenueAttributionManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 giugno 2026, 16:57 UTC
- Ora modificata: 30 giugno 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRevenueAttributionManagement`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RevenueAttributionCreation",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateRevenueAttribution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
```

```
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueAttributionListing",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListRevenueAttributions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueAttributionManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetRevenueAttribution",
        "partnercentral:UpdateRevenueAttribution"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
```

```
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRoboMaker_FullAccess

Descrizione: fornisce l'accesso completo AWS RoboMaker tramite Console di gestione AWS and SDK. Fornisce inoltre un accesso selezionato ai servizi correlati (ad esempio, S3, IAM).

`AWSRoboMaker_FullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSRoboMaker_FullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 settembre 2020, 18:34 UTC

- Ora modificata: 16 settembre 2021, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "robomaker:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr:BatchGetImage",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ecr-public:DescribeImages",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRoboMakerReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura AWS RoboMaker tramite Console di gestione AWS and SDK

`AWSRoboMakerReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSRoboMakerReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 novembre 2018, 05:30 UTC
- Ora modificata: 28 agosto 2020, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRoboMakerServicePolicy

Descrizione: politica RoboMaker del servizio

`AWSRoboMakerServicePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 novembre 2018, 06:30 UTC
- Ora modificata: 11 novembre 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction",
        "robomaker:CreateSimulationJob",
        "robomaker:CancelSimulationJob"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "robomaker:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:robomaker:*:*:simulation-job/*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration",
        "lambda:DeleteFunction",
        "lambda:ListVersionsByFunction",
        "lambda:GetAlias",
        "lambda:UpdateAlias",
        "lambda:CreateAlias",
        "lambda:DeleteAlias"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "robomaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRoboMakerServiceRolePolicy

Descrizione: politica RoboMaker del servizio

`AWSRoboMakerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSRoboMakerServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 novembre 2018, 05:33 UTC
- Ora modificata: 26 novembre 2018, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRolesAnywhereFullAccess

Descrizione: fornisce tutte le autorizzazioni per le risorse IAM Roles Anywhere, incluse ma non limitate a: CreateProfile,, DeleteTrustAnchor DisableCRL,. ResetNotificationSettings

`AWSRolesAnywhereFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSRolesAnywhereFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 luglio 2025, 14:52 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:CreateTrustAnchor",
        "rolesanywhere:DeleteTrustAnchor",
        "rolesanywhere:DisableTrustAnchor",
        "rolesanywhere:EnableTrustAnchor",
        "rolesanywhere:UpdateTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile",
        "rolesanywhere:CreateProfile",
        "rolesanywhere:DeleteProfile",
        "rolesanywhere:DisableProfile",
        "rolesanywhere:EnableProfile",
        "rolesanywhere:UpdateProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
```

```
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
        "rolesanywhere:GetCrl",
        "rolesanywhere:DeleteCrl",
        "rolesanywhere:DisableCrl",
        "rolesanywhere:EnableCrl",
        "rolesanywhere:ImportCrl",
        "rolesanywhere:UpdateCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
    {
      "Sid" : "OtherRolesAnywherePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:PutAttributeMapping",
        "rolesanywhere:DeleteAttributeMapping",
        "rolesanywhere:ResetNotificationSettings",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:TagResource",
        "rolesanywhere:UntagResource",
        "rolesanywhere:PutNotificationSettings"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PassRoleToRolesAnywhere",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "rolesanywhere.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateRolesAnywhereServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "rolesanywhere.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRolesAnywhereReadOnly

Descrizione: Fornisce autorizzazioni di sola lettura per le risorse IAM Roles Anywhere, inclusi ma non limitati a: GetTrustAnchor,, ListProfiles getCRL. Non ci saranno altre autorizzazioni per altri servizi inclusi in questa politica.

`AWSRolesAnywhereReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSRolesAnywhereReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 luglio 2025, 15:07 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
```

```
        "rolesanywhere:GetCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
      "Sid" : "Tags",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSRolesAnywhereServicePolicy

Descrizione: consente a IAM Roles Anywhere di pubblicare service/usage metriche CloudWatch e verificare lo stato delle autorità di certificazione private per tuo conto.

`AWSRolesAnywhereServicePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 5 luglio 2022, 15:26 UTC
- Ora modificata: 05 luglio 2022, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/RolesAnywhere",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSS3OnOutpostsServiceRolePolicy

Descrizione: consenti al servizio Amazon S3 on Outposts di gestire le risorse di rete EC2 per tuo conto.

`AWSS3OnOutpostsServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 03 ottobre 2023, 20:32 UTC
- Ora modificata: 03 ottobre 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeAddresses",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
      ],
```

```
      "Resource" : "*",
      "Sid" : "DescribeVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Sid" : "CreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForCreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:ipv4pool-ec2/*"
      ],
      "Sid" : "AllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForAllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "ReleaseVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "AllocateAddress"
          ],
          "aws:RequestTag/CreatedBy" : [
            "S3 On Outposts"
          ]
```

```
        }
      },
      "Sid" : "CreateTags"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSavingsPlansFullAccess

Descrizione: Fornisce l'accesso completo al servizio Savings Plans

`AWSSavingsPlansFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSavingsPlansFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 novembre 2019, 22:45 UTC
- Ora modificata: 6 novembre 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "savingsplans:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSavingsPlansReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura al servizio Savings Plans

`AWSSavingsPlansReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSavingsPlansReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 novembre 2019, 22:45 UTC
- Ora modificata: 6 novembre 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "savingsplans:Describe*",
        "savingsplans:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSDMPServiceRolePolicy

Descrizione: consenti a SDMP di creare e gestire risorse per conto del cliente.

`AWSSDMPServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 24 luglio 2026, 20:57 UTC
- Ora modificata: 24 luglio 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSDMPServiceRolePolicy`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/sdmp/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "AllowListOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels",
        "iam:ListPolicies",
        "iam:ListPolicyTags",
        "iam:ListRoles",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateRoleWithConditions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SDMP-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/AWSDenyAll"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:ResourceTag/CreatedBy" : "arn:aws:iam::*:role/SDMPServiceRole*"
        }
      }
    },
    {
      "Sid" : "AllowSDMPRoleTagging",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/SDMP-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedBy"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AttachAWSDenyAll",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/SDMP-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
        },
        "StringLike" : {
          "aws:ResourceTag/CreatedBy" : "arn:aws:iam::*:role/SDMPServiceRole*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadSDMPRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRoleTags",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SDMP-*",
        "arn:aws:iam::*:role/SDMPServiceRole*"
      ]
    },
    {
      "Sid" : "ReadSDMPPolicies",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:policy/SDMP*"
      ]
    },
    {
      "Sid" : "AllowSecurityServiceVerification",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ListDetectors",
        "guardduty:GetDetector",
        "macie2:GetMacieSession",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "securityhub:DescribeHub",
        "securityhub:ListFindingAggregators",
        "inspector2:BatchGetAccountStatus",
        "detective:ListGraphs",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecretsManagerClientReadOnlyAccess

Descrizione: Fornisce l'accesso per recuperare e descrivere segreti da Secrets Manager. Questa politica consente inoltre di decrittografare le chiavi KMS per i segreti di Secrets Manager.

`AWSSecretsManagerClientReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSSecretsManagerClientReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 novembre 2025, 20:04 UTC
- Ora modificata: 02 giugno 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecretsManagerClientReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerGetAndDescribeSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*"
    },
    {
      "Sid" : "SecretsManagerBatchGetSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:BatchGetSecretValue",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSDecryptKey",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityAgentServiceRolePolicy

Descrizione: consente a AWS Security Agent di gestire le risorse per tuo conto.

`AWSSecurityAgentServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 11 giugno 2026, 23:42 UTC
- Ora modificata: 11 giugno 2026, 23:42 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityAgentServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LatticeCreateResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeTagResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:TagResource"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "LatticeManageTaggedResourceGateways",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeleteResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeGetResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeApis",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateLatticeServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityAgentWebAppPolicy

Descrizione: fornisce le autorizzazioni agli utenti autenticati per accedere all'applicazione Web Security Agent per la configurazione e l'esecuzione di test automatici di penetrazione della sicurezza. Questa politica consente agli utenti di gestire i pentest, visualizzare i risultati, monitorare l'esecuzione dei test e interagire con AWS le risorse necessarie per le operazioni di test di sicurezza.

`AWSSecurityAgentWebAppPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSecurityAgentWebAppPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 febbraio 2026, 23:19 UTC
- Ora modificata: 11 giugno 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSecurityAgentWebAppPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListTargetDomains",
        "securityagent:BatchGetTargetDomains"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentSpaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:CreateThreat",
        "securityagent:BatchDeleteCodeReviews",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchDeleteThreatModels",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetCodeReviewJobs",
        "securityagent:BatchGetCodeReviewJobTasks",
        "securityagent:BatchGetCodeReviews",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentestJobTasks",
```

```
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetThreatModelJobs",
        "securityagent:BatchGetThreatModelJobTasks",
        "securityagent:BatchGetThreatModels",
        "securityagent:BatchGetThreats",
        "securityagent:CreateCodeReview",
        "securityagent:CreateDesignReview",
        "securityagent:CreatePentest",
        "securityagent:CreateThreatModel",
        "securityagent:DeleteArtifact",
        "securityagent:DeleteDesignReview",
        "securityagent:GetArtifact",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
        "securityagent:GetDesignReviewFeedback",
        "securityagent:ListArtifacts",
        "securityagent:ListCodeReviewJobsForCodeReview",
        "securityagent:ListCodeReviewJobTasks",
        "securityagent:ListCodeReviews",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentestJobTasks",
        "securityagent:ListPentests",
        "securityagent:ListThreatModelJobs",
        "securityagent:ListThreatModelJobTasks",
        "securityagent:ListThreatModels",
        "securityagent:ListThreats",
        "securityagent:PutDesignReviewFeedback",
        "securityagent:StartCodeRemediation",
        "securityagent:StartCodeReviewJob",
        "securityagent:StartPentestJob",
        "securityagent:StartThreatModelJob",
        "securityagent:StopCodeReviewJob",
        "securityagent:StopPentestJob",
        "securityagent:StopThreatModelJob",
        "securityagent:UpdateCodeReview",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest",
        "securityagent:UpdateThreat",
        "securityagent:UpdateThreatModel"
```

```
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityHubFullAccess

Descrizione: Fornisce l'accesso completo all'utilizzo di AWS Security Hub.

`AWSSecurityHubFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSecurityHubFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 23:54 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "securityhub.amazonaws.com",
            "securityhubv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:UpdateDetector",
        "guardduty:EnableOrganizationAdminAccount",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:DeleteDetector",
        "guardduty:CreateDetector",
        "guardduty:CreateMembers",
        "guardduty:UpdateOrganizationConfiguration",
        "guardduty:DescribeOrganizationConfiguration",
```

```
        "inspector2:BatchGetAccountStatus",
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:DisableDelegatedAdminAccount",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:UpdateOrganizationConfiguration",
        "inspector2:DescribeOrganizationConfiguration",
        "pricing:GetProducts",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityHubOrganizationsAccess

Descrizione: concede l'autorizzazione per abilitare e gestire AWS Security Hub all'interno di un'organizzazione. Include l'abilitazione del servizio in tutta l'organizzazione e la determinazione dell'account amministratore delegato per il servizio.

`AWSSecurityHubOrganizationsAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSecurityHubOrganizationsAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 marzo 2021, 20:53 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DescribeResourcePolicy"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
```

```
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource" : [
        "arn:aws:organizations::*:root/o-*/*",
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : [
            "SECURITYHUB_POLICY",
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:TagResource",
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityHubReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle risorse del AWS Security Hub

`AWSSecurityHubReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSecurityHubReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2018, 01:34 UTC
- Ora modificata: 22 febbraio 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
```

```
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityHubServiceRolePolicy

Descrizione: un ruolo collegato al servizio richiesto a AWS Security Hub per accedere alle tue risorse.

`AWSSecurityHubServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 27 novembre 2018, 23:47 UTC
- Ora modificata: 27 giugno 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Versione della politica

Versione della politica: v16 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "iam:GenerateCredentialReport",
        "organizations:ListAccounts",
        "config:PutEvaluations",
        "tag:GetResources",
        "iam:GetCredentialReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "securityhub:BatchDisableStandards",
        "securityhub:BatchEnableStandards",
        "securityhub:BatchUpdateStandardsControlAssociations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:CreateMembers",
        "securityhub:DeleteMembers",
```

```
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandards",
        "securityhub:DescribeStandardsControls",
        "securityhub:DisassociateFromAdministratorAccount",
        "securityhub:DisassociateMembers",
        "securityhub:DisableSecurityHub",
        "securityhub:EnableSecurityHub",
        "securityhub:GetEnabledStandards",
        "securityhub:ListStandardsControlAssociations",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:UpdateOrganizationConfiguration",
        "securityhub:UpdateSecurityControl",
        "securityhub:UpdateSecurityHubConfiguration",
        "securityhub:UpdateStandardsControl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceRoleConfigPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
    },
    {
      "Sid" : "SecurityHubServiceRoleOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "SecurityHubCSPMServiceRoleConfig",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:PutThirdPartyServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
*ConfigurationRecorderForSecurityHubCSPM*"
      ]
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleConfigListAndGet",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders",
        "config:GetConnector"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleIamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleConfigMetricsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityHubV2ServiceRolePolicy

Descrizione: questa policy consente a Security Hub di gestire le regole di AWS Config e le risorse di Security Hub nell'organizzazione e per conto dell'utente.

`AWSSecurityHubV2ServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 10 giugno 2025, 17:37 UTC
- Ora modificata: 27 giugno 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubV2ServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsConfig",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder",
        "config:PutThirdPartyServiceLinkedConfigurationRecorder"
      ],
      "Resource" : "arn:aws:config:*:*:configuration-recorder/
*ConfigurationRecorderForSecurityHubAssets*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsConfigListAndGet",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders",
        "config:GetConnector"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsIamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleSecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DisableSecurityHubV2",
        "securityhub:EnableSecurityHubV2",
```

```
        "securityhub:DescribeSecurityHubV2",
        "securityhub:EnableSecurityHubFeatureV2",
        "securityhub:DisableSecurityHubFeatureV2"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hubv2/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsOnResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsWithoutResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleDelegatedAdminPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleEcrListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaAndConfigMetricPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIamListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetAccountSummary"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2IamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/access-analyzer.amazonaws.com/
AWSServiceRoleForAccessAnalyzer"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "access-analyzer.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2ResAPermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CreateServiceLinkedAnalyzer",
        "access-analyzer:DeleteServiceLinkedAnalyzer"
      ],
      "Resource" : "arn:*:access-analyzer:*:*:analyzer/*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2ResAListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2APIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetFindingRecommendation",
        "access-analyzer:GenerateFindingRecommendation"
      ],
      "Resource" : "arn:*:access-analyzer:*:*:analyzer/
_AccessAnalyzerForSecurityHubV2*"
```

```
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAPIPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUserPolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*",
        "arn:aws:iam::*:user/*"
      ]
    },
    {
      "Sid" : "SecurityHubConnectorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:CreateConnector",
        "securityhub:UpdateConnector",
        "securityhub:DeleteConnector"
      ],
      "Resource" : "arn:aws:securityhub:*:*:connector/*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleInspectorConnectorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:CreateConnector",
        "inspector2:DeleteConnector",
        "inspector2:ListConnectors",
        "inspector2:ListConnectorScanConfigurations",
        "inspector2:UpdateConnector",
        "inspector2:UpdateConnectorScanConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLikeIfExists" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleInspectorIamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
thirdparty.inspector2.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "thirdparty.inspector2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOutboundIdentityFederationPermission",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "sts:IdentityTokenAudience" : [
            "api://AzureADTokenExchange"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityIncidentResponseCaseFullAccess

Descrizione: Policy fornisce ai clienti le autorizzazioni di lettura e scrittura per le risorse relative ai casi create tramite il servizio Security Incident Response.

`AWSSecurityIncidentResponseCaseFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSecurityIncidentResponseCaseFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2024, 23:21 UTC
- Ora modificata: 22 aprile 2026, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseCaseFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRCaseFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
```

```
        "security-ir:ListCaseEdits",
        "security-ir:CreateCase",
        "security-ir:UpdateCase",
        "security-ir:CloseCase",
        "security-ir:UpdateCaseStatus",
        "security-ir:UpdateResolverType",
        "security-ir:GetCaseAttachmentUploadUrl",
        "security-ir:CreateCaseComment",
        "security-ir:UpdateCaseComment",
        "security-ir:SendFeedback",
        "security-ir:ListInvestigations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIRCaseTagFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:ListTagsForResource",
        "security-ir:TagResource",
        "security-ir:UntagResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityIncidentResponseFullAccess

Descrizione: Policy fornisce ai clienti le autorizzazioni di lettura e scrittura per tutte le risorse associate al servizio Security Incident Response.

`AWSSecurityIncidentResponseFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSecurityIncidentResponseFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2024, 23:21 UTC
- Ora modificata: 22 aprile 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponse",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponseTriage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/triage.security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse_Triage"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityIncidentResponseReadOnlyAccess

Descrizione: Policy fornisce ai clienti Read-only le autorizzazioni per tutte le risorse associate al servizio Security Incident Response. L'autorizzazione include anche l'accesso alla GetCaseAttachmentDownloadUrl possibilità di ottenere gli URL per il download degli allegati dei casi.

`AWSSecurityIncidentResponseReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSecurityIncidentResponseReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2024, 23:06 UTC
- Ora modificata: 22 aprile 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetMembership",
        "security-ir:ListMemberships",
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:ListTagsForResource",
        "security-ir:ListInvestigations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityIncidentResponseServiceRolePolicy

Descrizione: fornisce l'accesso alle AWS risorse gestite o utilizzate da Security Incident Response

`AWSSecurityIncidentResponseServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 1 dicembre 2024, 16:36 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseServiceRolePolicy`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIncidentResponseOrganizationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SecurityIncidentResponseCreateCasePolicyTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:TagResource",
        "security-ir:CreateCase"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      },
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    },
    {
      "Sid" : "SecurityIncidentResponseOperationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:UpdateCase",
        "security-ir:ListCases",
        "security-ir:CreateCaseComment",
        "security-ir:ListComments"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSecurityIncidentResponseTriageServiceRolePolicy

Descrizione: fornisce l'accesso a AWS Security Incident Response per monitorare continuamente l'ambiente alla ricerca di minacce alla sicurezza, ottimizzare i servizi di sicurezza per ridurre il rumore degli avvisi e raccogliere informazioni per indagare su potenziali incidenti.

`AWSSecurityIncidentResponseTriageServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 1 dicembre 2024, 16:36 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseTriageServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
```

```
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:CreateFilter",
        "guardduty:DescribeMalwareScans",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:StartMalwareScan",
        "guardduty:UpdateFindingsFeedback"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:BatchUpdateFindings",
        "securityhub:DescribeHub",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindings",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:UpdateFindings"
```

```
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateCase",
        "security-ir:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:UpdateCase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetMembership",
        "security-ir:ListMemberships"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceCatalogAdminFullAccess

Descrizione: fornisce l'accesso completo alle funzionalità di amministrazione del catalogo dei servizi

`AWSServiceCatalogAdminFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSServiceCatalogAdminFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 febbraio 2018, 17:19 UTC
- Ora modificata: 13 aprile 2023, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateUploadBucket",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
```

```
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicecatalog:List*",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource",
        "servicecatalog:SyncResource",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:Accept*",
        "servicecatalog:Associate*",
        "servicecatalog:Batch*",
        "servicecatalog:Copy*",
        "servicecatalog:Create*",
        "servicecatalog:Delete*",
        "servicecatalog:Describe*",
        "servicecatalog:Disable*",
        "servicecatalog:Disassociate*",
        "servicecatalog:Enable*",
        "servicecatalog:Execute*",
        "servicecatalog:Import*",
        "servicecatalog:Provision*",
        "servicecatalog:Put*",
        "servicecatalog:Reject*",
        "servicecatalog:Terminate*",
        "servicecatalog:Update*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "servicecatalog.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
orgsdatasync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogOrgsDataSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "orgsdatasync.servicecatalog.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceCatalogAdminReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle funzionalità di amministrazione di Service Catalog

`AWSServiceCatalogAdminReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSServiceCatalogAdminReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 ottobre 2019, 18:53 UTC
- Ora modificata: 25 ottobre 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:List*",
        "servicecatalog:Describe*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:Search*",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceCatalogAppRegistryFullAccess

Descrizione: Fornisce l'accesso completo alle funzionalità del Service Catalog App Registry

`AWSServiceCatalogAppRegistryFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSServiceCatalogAppRegistryFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 novembre 2020, 22:25 UTC
- Ora modificata: 07 dicembre 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppRegistryUpdateStackAndResourceGroupTagging",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AppRegistryResourceGroupsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:GetGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:AssociateResource",
        "resource-groups:DisassociateResource"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/AWS_*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "servicecatalog:CreateApplication",
        "servicecatalog:GetApplication",
        "servicecatalog:UpdateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:AssociateResource",
        "servicecatalog:DisassociateResource",
```

```
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:CreateAttributeGroup",
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:SyncResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration",
        "servicecatalog:PutConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppRegistryResourceTagging",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListTagsForResource",
        "servicecatalog:UntagResource",
        "servicecatalog:TagResource"
      ],
      "Resource" : "arn:aws:servicecatalog:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceCatalogAppRegistryReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle funzionalità del registro delle app di Service Catalog

`AWSServiceCatalogAppRegistryReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSServiceCatalogAppRegistryReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 novembre 2020, 22:34 UTC
- Ora modificata: 17 novembre 2022, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:GetApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListTagsForResource",
        "servicecatalog:ListAttributeGroupsForApplication",
```

```
        "servicecatalog:GetConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceCatalogAppRegistryServiceRolePolicy

Descrizione: consente a Service Catalog AppRegistry di gestire Resource Groups per conto dell'utente

`AWSServiceCatalogAppRegistryServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 maggio 2021, 22:18 UTC
- Ora modificata: 26 ottobre 2022, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry*",
        "arn:*:resource-groups:*:*:group/AWS_CloudFormation_Stack*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceCatalogEndUserFullAccess

Descrizione: fornisce l'accesso completo alle funzionalità degli utenti finali del catalogo dei servizi

`AWSServiceCatalogEndUserFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSServiceCatalogEndUserFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 febbraio 2018, 17:22 UTC
- Ora modificata: 10 luglio 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:ValidateTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
```

```
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:CreateProvisionedProductPlan",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ExecuteProvisionedProductPlan",
        "servicecatalog:DeleteProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ExecuteProvisionedProductServiceAction",
        "servicecatalog:DescribeServiceActionExecutionParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
```

```
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceCatalogEndUserReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura alle funzionalità degli utenti finali di Service Catalog

`AWSServiceCatalogEndUserReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSServiceCatalogEndUserReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 ottobre 2019, 18:49 UTC
- Ora modificata: 25 ottobre 2019, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeServiceActionExecutionParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Descrizione: una policy Service Linked Role AWS ServiceCatalog per la sincronizzazione con la struttura organizzativa di AWS Organizations

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 aprile 2023, 20:48 UTC
- Ora modificata: 08 dicembre 2025, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "OrganizationsDataSyncToServiceCatalogRegions",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceCatalogSyncServiceRolePolicy

Descrizione: un ruolo collegato al servizio per AWS ServiceCatalog sincronizzare gli artifatti di provisioning dai repository di origine

`AWSServiceCatalogSyncServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 novembre 2022, 21:20 UTC
- Ora modificata: 03 maggio 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForAIDevOpsPolicy

Descrizione: questo ruolo collegato al servizio consente a AIDev Ops di fornire informazioni sull'utilizzo.

`AWSServiceRoleForAIDevOpsPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 16 febbraio 2026, 14:27 UTC
- Ora modificata: 27 marzo 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAIDevOpsPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AIDevOps"
          ]
        }
      }
    },
    {
      "Sid" : "LatticeCreateResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeTagResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:TagResource"
      ],
```

```
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeManageTaggedResourceGateways",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeleteResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeGetResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeApis",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CreateLatticeServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForAmazonEKSNodegroup

Descrizione: autorizzazioni necessarie per la gestione dei gruppi di nodi nell'account del cliente. Queste politiche riguardano la gestione delle seguenti risorse: AutoscalingGroups,, SecurityGroups e. LaunchTemplates InstanceProfiles

`AWSServiceRoleForAmazonEKSNodegroup`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 07 novembre 2019, 01:34 UTC
- Ora modificata: 17 febbraio 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "AutoscalingRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:PutLifecycleHook",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutWarmPool",
        "autoscaling:DeleteWarmPool"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
    },
    {
      "Sid" : "AllowAutoscalingToCreateSLR",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      },
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowASGCreationByEKS",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToAutoscaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToManageResourcesForNodegroups",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "ec2:CreateLaunchTemplate",
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "ec2:DescribeLaunchTemplates",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RunInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:GetConsoleOutput",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeCapacityReservations",
        "autoscaling:DescribeWarmPool"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
    },
    {
      "Sid" : "PermissionsToDeleteEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsForManagedNodegroupsAutoRepair",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "PermissionsToCreateEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*",
        "arn:*:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AllowTaggingEC2ResourcesOnlyDuringInstanceCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:instance/*",
        "arn:*:ec2:*:*:volume/*",
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForAmazonQDeveloper

Descrizione: questo ruolo collegato al servizio offre agli sviluppatori Amazon Q la capacità di fornire informazioni sull'utilizzo.

`AWSServiceRoleForAmazonQDeveloper`è una policy AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 25 aprile 2024, 07:40 UTC
- Ora modificata: 20 luglio 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

Versione della politica

Versione della politica: v2 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForAWSTransform

Descrizione: questo ruolo collegato ai servizi offre a AWS Transform la capacità di fornire informazioni sull'utilizzo.

`AWSServiceRoleForAWSTransform`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 maggio 2025, 13:37 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransform`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Transform"
          ]
        }
      }
    },
    {
      "Sid" : "UserManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:ListApplicationAssignmentsForPrincipal"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SupportCaseManagement",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:AddCommunicationToCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExternalIdpSecretsAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:transform!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "transform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForAWSTransformCustom

Descrizione: consente a AWS Transform Custom di pubblicare le CloudWatch metriche sul tuo account per tuo conto.

`AWSServiceRoleForAWSTransformCustom`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 25 marzo 2026, 02:57 UTC
- Ora modificata: 05 maggio 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransformCustom`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/TransformCustom"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/TransformCustom",
        "arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

Descrizione: Fornisce l'accesso alle risorse di Systems Manager utilizzate dagli CloudWatch allarmi

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 1 ottobre 2020, 09:49 UTC
- Ora modificata: 01 ottobre 2020, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

Descrizione: consente di accedere CloudWatch alle metriche di RDS Performance Insights per tuo conto

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 07 settembre 2023, 09:32 UTC
- Ora modificata: 07 settembre 2023, 09:32 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForCodeGuru-Profiler

Descrizione: un ruolo collegato al servizio richiesto ad Amazon CodeGuru Profiler per inviare notifiche per tuo conto.

`AWSServiceRoleForCodeGuru-Profiler`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 giugno 2020, 22:04 UTC
- Ora modificata: 26 giugno 2020, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForCodeWhispererPolicy

Descrizione: questo ruolo concede le autorizzazioni per accedere CodeWhisperer ai dati del tuo account per calcolare la fatturazione, fornisce l'accesso per creare e accedere ai report di sicurezza in Amazon e CodeGuru inviare dati a. CloudWatch

`AWSServiceRoleForCodeWhispererPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 24 marzo 2023, 19:39 UTC
- Ora modificata: 09 aprile 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance",
        "sso:DescribeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid3",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateUploadUrl"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid4",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:GetFindings"
      ],
      "Resource" : [
        "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
      ]
    },
    {
      "Sid" : "sid5",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/CodeWhisperer"
          ]
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForEC2ScheduledInstances

Descrizione: consente alle istanze pianificate EC2 di avviare e gestire le istanze spot.

`AWSServiceRoleForEC2ScheduledInstances`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 ottobre 2017, 18:31 UTC
- Ora modificata: 12 ottobre 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:ec2sri:scheduledInstanceId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2sri:scheduledInstanceId" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Descrizione: AWS GroundStation utilizza questo ruolo collegato al servizio per richiamare EC2 per trovare indirizzi pubblici IPv4

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 13 dicembre 2022, 23:52 UTC
- Ora modificata: 13 dicembre 2022, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForImageBuilder

Descrizione: consente di EC2ImageBuilder chiamare AWS i servizi per conto dell'utente.

`AWSServiceRoleForImageBuilder`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 29 novembre 2019, 22:02 UTC
- Ora modificata: 09 luglio 2026, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Versione della politica

Versione della politica: v28 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateLaunchTemplate",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeSnapshots",
        "ec2:DescribeHosts"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateImage"
          ],
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:AddTagsToResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListInventoryEntries",
        "ssm:SendAutomationSignal",
        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:DescribeAssociationExecutions",
```

```
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep",
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachImageWatermark"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "imagebuilder:StartImagePipelineExecution",
```

```
      "Resource" : "arn:aws:imagebuilder:*:*:image-pipeline/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "imagebuilder:TagResource",
      "Resource" : "arn:aws:imagebuilder:*:*:image-pipeline/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForIoTSiteWise

Descrizione: consente SiteWise all' AWS IoT di fornire e gestire gateway e interrogare i dati. La policy include le autorizzazioni AWS Greengrass necessarie per la distribuzione in gruppi, le autorizzazioni AWS Lambda per la creazione e l'aggiornamento di funzioni con prefisso di servizio e le autorizzazioni IoT AWS Analytics per l'interrogazione dei dati dai datastore.

`AWSServiceRoleForIoTSiteWise`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 novembre 2018, 19:19 UTC
- Ora modificata: 13 novembre 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ExecuteQuery"
      ],
      "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForLogDeliveryPolicy

Descrizione: consente al servizio Log Delivery di fornire i log chiamando la destinazione dei log per conto dell'utente.

`AWSServiceRoleForLogDeliveryPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 4 ottobre 2019, 17:31 UTC
- Ora modificata: 15 maggio 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogDeliveryToFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForMonitronPolicy

Descrizione: concede ad Amazon Monitron le autorizzazioni per AWS gestire le risorse, AWS inclusa l'assegnazione di utenti SSO per tuo conto.

`AWSServiceRoleForMonitronPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 2 dicembre 2020, 19:06 UTC
- Ora modificata: 07 gennaio 2026, 09:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:GetProfile",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:ListDirectoryAssociations",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "sso:CreateApplicationAssignment",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForNeptuneGraphPolicy

Descrizione: Fornisce l'accesso a Cloudwatch per pubblicare parametri e log operativi e di utilizzo per Amazon Neptune

`AWSServiceRoleForNeptuneGraphPolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 29 novembre 2023, 14:03 UTC
- Ora modificata: 29 novembre 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GraphMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Neptune",
            "AWS/Usage"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "GraphLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GraphLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForPrivateMarketplaceAdminPolicy

Descrizione: fornisce le autorizzazioni per descrivere e aggiornare le risorse di Private Marketplace e descrivere Organizations AWS

`AWSServiceRoleForPrivateMarketplaceAdminPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 febbraio 2024, 22:28 UTC
- Ora modificata: 14 febbraio 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceCatalogDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
```

```
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceStartChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "AssociateAudience",
            "DisassociateAudience"
          ]
        }
      },
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForProcurementInsightsPolicy

Descrizione: Policy for Procurement Insights per ottenere i dettagli dell'account dell'organizzazione

`AWSServiceRoleForProcurementInsightsPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 3 ottobre 2024, 14:26 UTC
- Ora modificata: 03 ottobre 2024, 14:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForProcurementInsightsPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProcurementInsightsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForSMS

Descrizione: fornisce l'accesso ai AWS servizi e alle risorse necessari per migrare le istanze di servizio AWS tra cui EC2, S3 e Cloudformation.

`AWSServiceRoleForSMS`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 6 agosto 2019, 18:39 UTC
- Ora modificata: 15 ottobre 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
```

```
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
```

```
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*",
```

```
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRoleForUserSubscriptions

Descrizione: fornisce l'accesso al servizio User Subscriptions alle risorse dell'Identity Center per aggiornare automaticamente le sottoscrizioni.

`AWSServiceRoleForUserSubscriptions`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 25 aprile 2024, 16:14 UTC
- Ora modificata: 22 giugno 2026, 08:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SubscriptionManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "organizations:DescribeOrganization",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso-directory:DescribeUser",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRolePolicyForBackupReports

Descrizione: Fornisce autorizzazioni di AWS Backup per creare report di conformità per tuo conto

`AWSServiceRolePolicyForBackupReports`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 19 agosto 2021, 21:16 UTC
- Ora modificata: 10 marzo 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeFramework",
        "backup:ListBackupJobs",
        "backup:ListRestoreJobs",
        "backup:ListCopyJobs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "config:DescribeConfigurationAggregators",
        "config:SelectAggregateResourceConfig",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "s3:GetBucketLocation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/
backup.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator"
      ],
      "Resource" : "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
backup.amazonaws.com*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRolePolicyForBackupRestoreTesting

Descrizione: questa politica contiene le autorizzazioni per testare i ripristini e per ripulire le risorse create durante i test.

`AWSServiceRolePolicyForBackupRestoreTesting`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 novembre 2023, 23:37 UTC
- Ora modificata: 18 marzo 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BackupActions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRestoreJob",
        "backup:DescribeProtectedResource",
        "backup:GetRecoveryPointRestoreMetadata",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByResource",
        "backup:ListTags",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IamPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:TerminateInstances",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:DeleteMountTarget",
        "rds:DeleteDBCluster",
        "rds:DeleteDBInstance",
        "rds:DeleteTenantDatabase",
        "fsx:DeleteFileSystem",
```

```
        "fsx:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/awsbackup-restore-test" : "false"
        }
      }
    },
    {
      "Sid" : "DdbDeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDeleteActions",
      "Effect" : "Allow",
      "Action" : "redshift:DeleteCluster",
      "Resource" : "arn:aws:redshift:*:*:cluster:awsbackup-restore-test-*"
    },
    {
      "Sid" : "S3DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "TimestreamDeleteActions",
      "Effect" : "Allow",
      "Action" : "timestream:DeleteTable",
      "Resource" : "arn:aws:timestream:*:*:database/*/table/awsbackup-restore-test-*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSServiceRolePolicyForWorkspacesInstances

Descrizione: questa policy gestita fornisce l'accesso amministrativo ad Amazon WorkSpaces per gestire le istanze EC2 nel tuo Account AWS

`AWSServiceRolePolicyForWorkspacesInstances`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 11 giugno 2025, 20:37 UTC
- Ora modificata: 29 giugno 2026, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForWorkspacesInstances`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateCapacityReservation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateCapacityReservation",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ManagedBy" : "workspaces-instances"
        }
      }
    },
    {
      "Sid" : "ManageTaggedCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyCapacityReservation",
        "ec2:CancelCapacityReservation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedBy" : "workspaces-instances"
```

```
        }
      }
    },
    {
      "Sid" : "TagRemediation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:capacity-reservation/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ManagedBy" : "workspaces-instances"
        }
      }
    },
    {
      "Sid" : "ManagedInstanceOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ManagedResourceOperator" : "workspaces-instances.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSShieldDRTAccessPolicy

Descrizione: fornisce allo AWS DDo S Response Team un accesso limitato alle vostre risorse per aiutarvi Account AWS a mitigare DDo gli attacchi S durante un evento di elevata gravità.

`AWSShieldDRTAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSShieldDRTAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 5 giugno 2018, 22:29 UTC
- Ora modificata: 15 dicembre 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SRTAccessProtectedResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:List*",
        "route53:List*",
        "elasticloadbalancing:Describe*",
        "cloudwatch:Describe*",
```

```
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SRTManageProtections",
      "Effect" : "Allow",
      "Action" : [
        "shield:*",
        "waf:*",
        "wafv2:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "cloudfront:UpdateDistribution",
        "apigateway:SetWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSShieldServiceRolePolicy

Descrizione: consente a AWS Shield di accedere alle AWS risorse per tuo conto per fornire protezione DDo S.

`AWSShieldServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 novembre 2021, 19:17 UTC
- Ora modificata: 17 novembre 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSocialMessagingServiceRolePolicy

Descrizione: fornisce l'accesso alle metriche di pubblicazione e fornisce informazioni dettagliate per l'invio di messaggi sui social.

`AWSSocialMessagingServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 ottobre 2024, 19:28 UTC
- Ora modificata: 10 ottobre 2024, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSocialMessagingServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchMetricPublishing",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SocialMessaging"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSSMForSAPServiceLinkedRolePolicy

Descrizione: fornisce a AWS Systems Manager for SAP le autorizzazioni necessarie per gestire e integrare il software SAP con. AWS

`AWSSSMForSAPServiceLinkedRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 16 novembre 2022, 01:18 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v21 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:*:events:*:*:rule/SSMSAPManagedRule*",
        "arn:*:events:*:*:event-bus/default"
      ]
    },
    {
      "Sid" : "DocumentActions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
        "arn:*:ssm:*:*:document/AWSSSMSAP*",
        "arn:*:ssm:*:*:document/AWSSAP*"
      ]
    },
    {
      "Sid" : "CustomerSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ssm:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "InstanceTagActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/awsApplication" : "false"
        },
        "StringEqualsIgnoreCase" : {
          "ec2:ResourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "DescribeTag",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeTags",
      "Resource" : "*"
    },
    {
      "Sid" : "GetApplication",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetApplication",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "UpdateOrDeleteApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DeleteApplication",
        "servicecatalog:UpdateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TagResource",
        "servicecatalog:CreateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/SSMForSAP"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:CreateAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "GetAttributeGroup",
      "Effect" : "Allow",
```

```
      "Action" : "servicecatalog:GetAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
    },
    {
      "Sid" : "DeleteAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:DeleteAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "AttributeGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "ListAssociatedAttributeGroups",
      "Effect" : "Allow",
      "Action" : "servicecatalog:ListAssociatedAttributeGroups",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "CreateGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "GetGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:GetGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
    },
    {
      "Sid" : "DeleteGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "TagAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag"
```

```
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "GetAppTagResourceGroupConfig",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
      ]
    },
    {
      "Sid" : "StartStopInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "SsmSapResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag",
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEc2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPManaged" : "True"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageAppTagsOnEbsVolumes",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/awsApplication" : "arn:aws:resource-groups:*:*:group/*/*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "awsApplication"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCostAllocationTags",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:StartCostAllocationTagBackfill"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSSMOpsInsightsServiceRolePolicy

Descrizione: Policy for Service Linked Role AWSServiceRoleForAmazonSSM_OpsInsights

`AWSSSMOpsInsightsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 16 giugno 2021, 20:12 UTC
- Ora modificata: 16 giugno 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:UpdateOpsItem",
        "ssm:GetOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SsmOperationalInsight" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSSODirectoryAdministrator

Descrizione: accesso da amministratore per SSO Directory

`AWSSSODirectoryAdministrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSSODirectoryAdministrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 31 ottobre 2018, 23:54 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSSODirectoryReadOnly

Descrizione: ReadOnly accesso per SSO Directory

`AWSSSODirectoryReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSSODirectoryReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 31 ottobre 2018, 23:49 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:Search*",
```

```
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Get*",
        "identitystore:Describe*",
        "identitystore:List*",
        "identitystore-auth:ListSessions",
        "identitystore-auth:BatchGetSession"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSSOMasterAccountAdministrator

Descrizione: Fornisce l'accesso all'interno dell' AWS SSO per gestire gli account master e membri di AWS Organizations e l'applicazione cloud

`AWSSSOMasterAccountAdministrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSSOMasterAccountAdministrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2018, 20:36 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSSOMemberAccountAdministrator

Descrizione: Fornisce l'accesso all'interno dell' AWS SSO per gestire gli account dei membri di AWS Organizations e l'applicazione cloud

`AWSSSOMemberAccountAdministrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSSOMemberAccountAdministrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2018, 20:45 UTC

- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
```

```
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSSOReadOnly

Descrizione: fornisce accesso in sola lettura alle configurazioni AWS SSO.

`AWSSSOReadOnly` è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSSOReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2018, 20:24 UTC

- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOReadOnly`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSSOServiceRolePolicy

Descrizione: concede le autorizzazioni AWS SSO per gestire le AWS risorse, inclusi ruoli IAM, policy e IdP SAML per tuo conto.

`AWSSSOServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 5 dicembre 2017, 18:36 UTC
- Ora modificata: 11 febbraio 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Versione della politica

Versione della politica: v18 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
```

```
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMRoleReadActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMRoleCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "IAMSLRCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
      ]
```

```
    },
    {
      "Sid" : "IAMSAMLProviderCreationAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMSAMLProviderUpdateAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSAMLProvider",
        "iam:GetSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
```

```
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowUnauthAppForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:UnauthorizeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
```

```
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSStepFunctionsConsoleFullAccess

Descrizione: una politica di accesso per fornire un user/role/etc accesso alla AWS StepFunctions console. Per un'esperienza completa con la console, oltre a questa policy, un utente potrebbe aver bisogno di iam: PassRole autorizzazione per altri ruoli IAM che può essere assunta dal servizio.

`AWSStepFunctionsConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSStepFunctionsConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 gennaio 2017, 21:54 UTC
- Ora modificata: 12 gennaio 2017, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/StatesExecutionRole*"
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:ListFunctions",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSStepFunctionsFullAccess

Descrizione: una politica di accesso per fornire un user/role/etc accesso all' AWS StepFunctions API. Per un accesso completo, oltre a questa politica, un utente DEVE disporre di iam: PassRole autorizzazione su almeno un ruolo IAM che può essere assunto dal servizio.

`AWSStepFunctionsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSStepFunctionsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 gennaio 2017, 21:51 UTC
- Ora modificata: 11 gennaio 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSStepFunctionsReadOnlyAccess

Descrizione: una politica di accesso per fornire un accesso in sola user/role/etc lettura al AWS StepFunctions servizio.

`AWSStepFunctionsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSStepFunctionsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 gennaio 2017, 21:46 UTC
- Ora modificata: 26 aprile 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:ListActivities",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineForExecution",
        "states:ListExecutions",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:DescribeActivity",
        "states:ListTagsForResource",
        "states:DescribeMapRun",
        "states:ListMapRuns",
        "states:DescribeStateMachineAlias",
        "states:ListStateMachineAliases",
        "states:ListStateMachineVersions",
        "states:ValidateStateMachineDefinition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSStorageGatewayFullAccess

Descrizione: fornisce l'accesso completo a AWS Storage Gateway tramite Console di gestione AWS.

`AWSStorageGatewayFullAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSStorageGatewayFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 06 settembre 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSStorageGatewayReadOnlyAccess

Descrizione: fornisce l'accesso a AWS Storage Gateway tramite Console di gestione AWS.

`AWSStorageGatewayReadOnlyAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSStorageGatewayReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 06 settembre 2022, 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSStorageGatewayServiceRolePolicy

Descrizione: ruolo collegato ai servizi utilizzato da AWS Storage Gateway per consentire l'integrazione di altri AWS servizi con Storage Gateway.

`AWSStorageGatewayServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 febbraio 2021, 19:03 UTC
- Ora modificata: 17 febbraio 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
```

```
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSupplyChainFederationAdminAccess

Descrizione: AWSSupply ChainFederationAdminAccess fornisce agli utenti federati di AWS Supply Chain l'accesso all'applicazione AWS Supply Chain, incluse le autorizzazioni necessarie per eseguire azioni all'interno dell'applicazione AWS Supply Chain. La policy fornisce autorizzazioni amministrative per gli utenti e i gruppi di IAM Identity Center ed è associata a un ruolo creato da AWS Supply Chain per tuo conto. Non dovresti collegare la AWSSupply ChainFederationAdminAccess policy a nessun'altra entità IAM.

`AWSSupplyChainFederationAdminAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSupplyChainFederationAdminAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 1 marzo 2023, 18:54 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime:DeleteChannelMembership",
        "chime:DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",
        "chime:SendChannelMessage",
        "chime:UpdateChannelReadMarker",
        "chime:UpdateAppInstanceUser"
      ],
```

```
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SCNInstanceId" : "*"
        }
      }
    },
    {
      "Sid" : "ChimeChannel",
      "Effect" : "Allow",
      "Action" : [
        "chime:DescribeChannel"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ]
    },
    {
      "Sid" : "ChimeMessaging",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMessagingSessionEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:ListDirectoryAssociations",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso:ListApplicationAssignments",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:GetApplicationAssignmentConfiguration"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AppflowConnectorProfile",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateConnectorProfile",
        "appflow:UseConnectorProfile",
        "appflow:DeleteConnectorProfile",
        "appflow:UpdateConnectorProfile"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:connectorprofile/scn-*"
      ]
    },
    {
      "Sid" : "AppflowFlow",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateFlow",
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow",
        "appflow:TagResource",
        "appflow:UntagResource"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:flow/scn-*"
      ]
    },
    {
      "Sid" : "S3ListAllBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListSupplyChainBucket",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ]
    },
    {
      "Sid" : "S3ReadWriteObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicy",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "KMSListKeys",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSListGrants",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "KMSCreateGrant",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSupportAccess

Descrizione: consente agli utenti di accedere al Supporto AWS Centro.

`AWSSupportAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSupportAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*",
        "support-console:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSupportAppFullAccess

Descrizione: Fornisce l'accesso completo all' Supporto AWS App e ad altri servizi richiesti, come Supporto AWS Service Quotas. Questa politica include le autorizzazioni per utilizzare i servizi di supporto in modo che l'utente possa contattarli Supporto AWS per casi di assistenza, modificare le quote di servizio e creare i ruoli pertinenti collegati ai servizi.

`AWSSupportAppFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSSupportAppFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 agosto 2022, 16:53 UTC
- Ora modificata: 22 agosto 2022, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:RequestServiceQuotaIncrease",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeSeverityLevels",
        "support:InitiateChatForCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSupportAppReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura all' Supporto AWS app.

`AWSSupportAppReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSupportAppReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 agosto 2022, 17:01 UTC
- Ora modificata: 22 agosto 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSupportPlansFullAccess

Descrizione: fornisce l'accesso completo ai piani di supporto.

`AWSSupportPlansFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSupportPlansFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 settembre 2022, 18:19 UTC
- Ora modificata: 09 settembre 2024, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSupportPlansReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ai piani di supporto.

`AWSSupportPlansReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSSupportPlansReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 settembre 2022, 18:08 UTC
- Ora modificata: 09 settembre 2024, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
```

```
        "supportplans:ListSupportPlanModifiers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSupportPlansServiceRolePolicy

Descrizione: consente ai Supporto AWS piani di leggere e aggiornare AWS le risorse utilizzate per gestire il piano di supporto del tuo account per tuo conto.

`AWSSupportPlansServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 31 luglio 2026, 17:12 UTC
- Ora modificata: 31 luglio 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportPlansServiceRolePolicy`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:AcceptSupportAgreement",
        "supportplans:CancelSupportAgreement",
        "supportplans:CreateSupportAgreement",
        "supportplans:GetSupportAgreement",
        "supportplans:ListSupportAgreements",
        "supportplans:ListSupportAgreementRevisions",
        "supportplans:RejectSupportAgreement",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:UpdateSupportAgreement",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSupportServiceRolePolicy

Descrizione: consente di accedere Supporto AWS alle AWS risorse per fornire servizi di fatturazione, amministrazione e supporto.

`AWSSupportServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 19 aprile 2018, 18:04 UTC
- Ora modificata: 22 giugno 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Versione della politica

Versione della politica: v58 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
```

```
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
```

```
    {
      "Sid" : "AWSSupportDeleteRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:getAccessPreview",
        "access-analyzer:getAnalyzedResource",
        "access-analyzer:getAnalyzer",
        "access-analyzer:getArchiveRule",
        "access-analyzer:getFinding",
        "access-analyzer:getGeneratedPolicy",
        "access-analyzer:listAccessPreviewFindings",
        "access-analyzer:listAccessPreviews",
        "access-analyzer:listAnalyzedResources",
        "access-analyzer:listAnalyzers",
        "access-analyzer:listArchiveRules",
        "access-analyzer:listFindings",
        "access-analyzer:listPolicyGenerations",
        "account:getRegionOptStatus",
        "account:listRegions",
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "acm:searchCertificates",
        "aidevops:describePrivateConnection",
```

```
        "aidevops:getAccountUsage",
        "aidevops:getAgentSpace",
        "aidevops:getAssociation",
        "aidevops:getBacklogTask",
        "aidevops:getOperatorApp",
        "aidevops:getRecommendation",
        "aidevops:getService",
        "aidevops:listAgentSpaces",
        "aidevops:listAssociations",
        "aidevops:listBacklogTasks",
        "aidevops:listChats",
        "aidevops:listExecutions",
        "aidevops:listGoals",
        "aidevops:listPrivateConnections",
        "aidevops:listRecommendations",
        "aidevops:listServices",
        "aidevops:listWebHooks",
        "aiops:getInvestigationGroup",
        "aiops:getInvestigationGroupPolicy",
        "aiops:listInvestigationGroups",
        "airflow-serverless:getTaskInstance",
        "airflow-serverless:getWorkflow",
        "airflow-serverless:getWorkflowRun",
        "airflow-serverless:listTaskInstances",
        "airflow-serverless:listWorkflowRuns",
        "airflow-serverless:listWorkflows",
        "airflow-serverless:listWorkflowVersions",
        "airflow:getEnvironment",
        "airflow:listEnvironments",
        "airflow:listTagsForResource",
        "amplify:getApp",
        "amplify:getBackendEnvironment",
        "amplify:getBranch",
        "amplify:getDomainAssociation",
        "amplify:getJob",
        "amplify:getWebhook",
        "amplify:listApps",
        "amplify:listBackendEnvironments",
        "amplify:listBranches",
        "amplify:listDomainAssociations",
        "amplify:listJobs",
        "amplify:listResourcesForWebACL",
        "amplify:listWebhooks",
        "amplifyuibuilder:exportComponents",
```

```
        "amplifyuibuilder:exportThemes",
        "apigateway:getPortal",
        "apigateway:getPortalProduct",
        "apigateway:getPortalProductSharingPolicy",
        "apigateway:getProductPage",
        "apigateway:getProductRestEndpointPage",
        "apigateway:getRoutingRule",
        "apigateway:listPortalProducts",
        "apigateway:listPortals",
        "apigateway:listProductPages",
        "apigateway:listProductRestEndpointPages",
        "apigateway:listRoutingRules",
        "aoss:batchGetCollection",
        "aoss:batchGetCollectionGroup",
        "aoss:batchGetEffectiveLifecyclePolicy",
        "aoss:batchGetLifecyclePolicy",
        "aoss:batchGetVpcEndpoint",
        "aoss:getAccessPolicy",
        "aoss:getAccountSettings",
        "aoss:getIndex",
        "aoss:getPoliciesStats",
        "aoss:getSecurityConfig",
        "aoss:getSecurityPolicy",
        "aoss:listAccessPolicies",
        "aoss:listCollectionGroups",
        "aoss:listCollections",
        "aoss:listLifecyclePolicies",
        "aoss:listSecurityConfigs",
        "aoss:listSecurityPolicies",
        "aoss:listTagsForResource",
        "aoss:listVpcEndpoints",
        "appconfig:getApplication",
        "appconfig:getConfigurationProfile",
        "appconfig:getDeployment",
        "appconfig:getDeploymentStrategy",
        "appconfig:getEnvironment",
        "appconfig:getExtension",
        "appconfig:getExtensionAssociation",
        "appconfig:listApplications",
        "appconfig:listConfigurationProfiles",
        "appconfig:listDeployments",
        "appconfig:listDeploymentStrategies",
        "appconfig:listEnvironments",
        "appconfig:listExtensionAssociations",
```

```
        "appconfig:listExtensions",
        "appconfig:listHostedConfigurationVersions",
        "appflow:describeConnectorEntity",
        "appflow:describeConnectorProfiles",
        "appflow:describeConnectors",
        "appflow:describeFlow",
        "appflow:describeFlowExecutionRecords",
        "appflow:listConnectorEntities",
        "appflow:listFlows",
        "application-autoscaling:describeScalableTargets",
        "application-autoscaling:describeScalingActivities",
        "application-autoscaling:describeScalingPolicies",
        "application-autoscaling:describeScheduledActions",
        "application-signals:getService",
        "application-signals:getServiceLevelObjective",
        "application-signals:listServiceDependencies",
        "application-signals:listServiceDependents",
        "application-signals:listServiceLevelObjectives",
        "application-signals:listServiceOperations",
        "application-signals:listServices",
        "applicationinsights:describeApplication",
        "applicationinsights:describeComponent",
        "applicationinsights:describeComponentConfiguration",
        "applicationinsights:describeComponentConfigurationRecommendation",
        "applicationinsights:describeLogPattern",
        "applicationinsights:describeObservation",
        "applicationinsights:describeProblem",
        "applicationinsights:describeProblemObservations",
        "applicationinsights:listApplications",
        "applicationinsights:listComponents",
        "applicationinsights:listConfigurationHistory",
        "applicationinsights:listLogPatterns",
        "applicationinsights:listLogPatternSets",
        "applicationinsights:listProblems",
        "appmesh:describeGatewayRoute",
        "appmesh:describeMesh",
        "appmesh:describeRoute",
        "appmesh:describeVirtualGateway",
        "appmesh:describeVirtualNode",
        "appmesh:describeVirtualRouter",
        "appmesh:describeVirtualService",
        "appmesh:listGatewayRoutes",
        "appmesh:listMeshes",
        "appmesh:listRoutes",
```

```
        "appmesh:listTagsForResource",
        "appmesh:listVirtualGateways",
        "appmesh:listVirtualNodes",
        "appmesh:listVirtualRouters",
        "appmesh:listVirtualServices",
        "apprunner:describeAutoScalingConfiguration",
        "apprunner:describeCustomDomains",
        "apprunner:describeObservabilityConfiguration",
        "apprunner:describeOperation",
        "apprunner:describeService",
        "apprunner:describeVpcConnector",
        "apprunner:describeVpcIngressConnection",
        "apprunner:listAutoScalingConfigurations",
        "apprunner:listConnections",
        "apprunner:listObservabilityConfigurations",
        "apprunner:listOperations",
        "apprunner:listAssociatedServicesForWebAcl",
        "apprunner:listServices",
        "apprunner:listTagsForResource",
        "apprunner:listVpcConnectors",
        "apprunner:listVpcIngressConnections",
        "appstream:describeAppBlockBuilderAppBlockAssociations",
        "appstream:describeAppBlockBuilders",
        "appstream:describeAppBlocks",
        "appstream:describeApplicationFleetAssociations",
        "appstream:describeApplications",
        "appstream:describeDirectoryConfigs",
        "appstream:describeEntitlements",
        "appstream:describeFleets",
        "appstream:describeImageBuilders",
        "appstream:describeImagePermissions",
        "appstream:describeImages",
        "appstream:describeSessions",
        "appstream:describeStacks",
        "appstream:describeUsageReportSubscriptions",
        "appstream:describeUsers",
        "appstream:describeUserStackAssociations",
        "appstream:listAssociatedFleets",
        "appstream:listAssociatedStacks",
        "appstream:listEntitledApplications",
        "appstream:listTagsForResource",
        "appsync:evaluateCode",
        "appsync:evaluateMappingTemplate",
        "appsync:getApi",
```

```
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getChannelNamespace",
        "appsync:getDataSource",
        "appsync:getDataSourceIntrospection",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "appsync:getGraphqlApiEnvironmentVariables",
        "appsync:getIntrospectionSchema",
        "appsync:getResolver",
        "appsync:getSchemaCreationStatus",
        "appsync:getSourceApiAssociation",
        "appsync:getType",
        "appsync:listApis",
        "appsync:listChannelNamespaces",
        "appsync:listDataSources",
        "appsync:listDomainNames",
        "appsync:listFunctions",
        "appsync:listGraphqlApis",
        "appsync:listResolvers",
        "appsync:listResolversByFunction",
        "appsync:listSourceApiAssociations",
        "appsync:listTypes",
        "appsync:listTypesByAssociation",
        "aps:describeAlertManagerDefinition",
        "aps:describeRuleGroupsNamespace",
        "aps:describeScraper",
        "aps:describeWorkspace",
        "aps:listRuleGroupsNamespaces",
        "aps:listScrapers",
        "aps:listWorkspaces",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getCapacityAssignmentConfiguration",
        "athena:getCapacityReservation",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
```

```
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listCapacityReservations",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "auditmanager:getAccountStatus",
        "auditmanager:getDelegations",
        "auditmanager:listAssessmentFrameworks",
        "auditmanager:listAssessmentReports",
        "auditmanager:listAssessments",
        "auditmanager:listControls",
        "auditmanager:listKeywordsForDataSource",
        "auditmanager:listNotifications",
        "autoscaling-plans:describeScalingPlanResources",
        "autoscaling-plans:describeScalingPlans",
        "autoscaling-plans:getScalingPlanResourceForecastData",
        "autoscaling:describeAccountLimits",
        "autoscaling:describeAdjustmentTypes",
        "autoscaling:describeAutoScalingGroups",
        "autoscaling:describeAutoScalingInstances",
        "autoscaling:describeAutoScalingNotificationTypes",
        "autoscaling:describeInstanceRefreshes",
        "autoscaling:describeLaunchConfigurations",
        "autoscaling:describeLifecycleHooks",
        "autoscaling:describeLifecycleHookTypes",
        "autoscaling:describeLoadBalancers",
        "autoscaling:describeLoadBalancerTargetGroups",
        "autoscaling:describeMetricCollectionTypes",
        "autoscaling:describeNotificationConfigurations",
        "autoscaling:describePolicies",
        "autoscaling:describeScalingActivities",
        "autoscaling:describeScalingProcessTypes",
        "autoscaling:describeScheduledActions",
        "autoscaling:describeTags",
```

```
        "autoscaling:describeTerminationPolicyTypes",
        "autoscaling:describeTrafficSources",
        "autoscaling:describeWarmPool",
        "aws-marketplace:describeAgreement",
        "aws-marketplace:describeEntity",
        "aws-marketplace:listEntities",
        "aws-marketplace:searchAgreements",
        "backup-gateway:getBandwidthRateLimitSchedule",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup-search:listSearchJobBackups",
        "backup-search:listSearchJobs",
        "backup:describeScanJob",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRecoveryPointIndexDetails",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:getTieringConfiguration",
```

```
        "backup:listBackupJobs",
        "backup:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listIndexedRecoveryPoints",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listScanJobSummaries",
        "backup:listScanJobs",
        "backup:listTags",
        "backup:listTieringConfigurations",
        "batch:describeComputeEnvironments",
        "batch:describeConsumableResource",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
        "batch:describeSchedulingPolicies",
        "batch:describeServiceEnvironments",
        "batch:describeServiceJob",
        "batch:getJobQueueSnapshot",
        "batch:listConsumableResources",
        "batch:listJobs",
        "batch:listJobsByConsumableResource",
        "batch:listSchedulingPolicies",
        "batch:listServiceJobs",
        "batch:listTagsForResource",
        "bedrock:exportAutomatedReasoningPolicyVersion",
        "bedrock:getAgent",
        "bedrock:getAgentActionGroup",
        "bedrock:getAgentAlias",
        "bedrock:getAgentKnowledgeBase",
```

```
        "bedrock:getAgentMemory",
        "bedrock:getAgentVersion",
        "bedrock:getAsyncInvoke",
        "bedrock:getAutomatedReasoningPolicy",
        "bedrock:getAutomatedReasoningPolicyAnnotations",
        "bedrock:getAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:getAutomatedReasoningPolicyBuildWorkflowResultAssets",
        "bedrock:getAutomatedReasoningPolicyNextScenario",
        "bedrock:getAutomatedReasoningPolicyTestCase",
        "bedrock:getAutomatedReasoningPolicyTestResult",
        "bedrock:getBlueprint",
        "bedrock:getCustomModel",
        "bedrock:getCustomModelDeployment",
        "bedrock:getDataAutomationProject",
        "bedrock:getDataAutomationStatus",
        "bedrock:getDataSource",
        "bedrock:getEvaluationJob",
        "bedrock:getExecutionFlowSnapshot",
        "bedrock:getFlow",
        "bedrock:getFlowAlias",
        "bedrock:getFlowExecution",
        "bedrock:getFlowVersion",
        "bedrock:getFoundationModel",
        "bedrock:getFoundationModelAvailability",
        "bedrock:getGuardrail",
        "bedrock:getImportedModel",
        "bedrock:getInferenceProfile",
        "bedrock:getIngestionJob",
        "bedrock:getInvocationStep",
        "bedrock:getKnowledgeBase",
        "bedrock:getMarketplaceModelEndpoint",
        "bedrock:getModelCopyJob",
        "bedrock:getModelCustomizationJob",
        "bedrock:getModelImportJob",
        "bedrock:getModelInvocationJob",
        "bedrock:getModelInvocationLoggingConfiguration",
        "bedrock:getPrompt",
        "bedrock:getPromptRouter",
        "bedrock:getProvisionedModelThroughput",
        "bedrock:getSession",
        "bedrock:getUseCaseForModelAccess",
        "bedrock:listAgentActionGroups",
        "bedrock:listAgentAliases",
        "bedrock:listAgentKnowledgeBases",
```

```
        "bedrock:listAgents",
        "bedrock:listAgentVersions",
        "bedrock:listAsyncInvokes",
        "bedrock:listAutomatedReasoningPolicies",
        "bedrock:listAutomatedReasoningPolicyBuildWorkflows",
        "bedrock:listAutomatedReasoningPolicyTestCases",
        "bedrock:listAutomatedReasoningPolicyTestResults",
        "bedrock:listBlueprints",
        "bedrock:listCustomModelDeployments",
        "bedrock:listCustomModels",
        "bedrock:listDataAutomationProjects",
        "bedrock:listDataSources",
        "bedrock:listEnforcedGuardrailsConfiguration",
        "bedrock:listEvaluationJobs",
        "bedrock:listFlowAliases",
        "bedrock:listFlowExecutionEvents",
        "bedrock:listFlowExecutions",
        "bedrock:listFlows",
        "bedrock:listFlowVersions",
        "bedrock:listFoundationModelAgreementOffers",
        "bedrock:listFoundationModels",
        "bedrock:listGuardrails",
        "bedrock:listImportedModels",
        "bedrock:listInferenceProfiles",
        "bedrock:listIngestionJobs",
        "bedrock:listInvocationSteps",
        "bedrock:listKnowledgeBases",
        "bedrock:listMarketplaceModelEndpoints",
        "bedrock:listModelCopyJobs",
        "bedrock:listModelCustomizationJobs",
        "bedrock:listModelImportJobs",
        "bedrock:listModelInvocationJobs",
        "bedrock:listPromptRouters",
        "bedrock:listPrompts",
        "bedrock:listProvisionedModelThroughputs",
        "bedrock:listSessions",
        "bedrock-agentcore:getAgentCard",
        "bedrock-agentcore:getAgentRuntime",
        "bedrock-agentcore:getAgentRuntimeEndpoint",
        "bedrock-agentcore:getApiKeyCredentialProvider",
        "bedrock-agentcore:getBrowser",
        "bedrock-agentcore:getBrowserSession",
        "bedrock-agentcore:getCodeInterpreter",
        "bedrock-agentcore:getCodeInterpreterSession",
```

```
        "bedrock-agentcore:getEvaluator",
        "bedrock-agentcore:getEvent",
        "bedrock-agentcore:getGateway",
        "bedrock-agentcore:getGatewayTarget",
        "bedrock-agentcore:getMemory",
        "bedrock-agentcore:getMemoryRecord",
        "bedrock-agentcore:getOauth2CredentialProvider",
        "bedrock-agentcore:getOnlineEvaluationConfig",
        "bedrock-agentcore:getPolicy",
        "bedrock-agentcore:getPolicyEngine",
        "bedrock-agentcore:getPolicyGeneration",
        "bedrock-agentcore:getResourcePolicy",
        "bedrock-agentcore:getTokenVault",
        "bedrock-agentcore:getWorkloadIdentity",
        "bedrock-agentcore:listActors",
        "bedrock-agentcore:listAgentRuntimeEndpoints",
        "bedrock-agentcore:listAgentRuntimeVersions",
        "bedrock-agentcore:listAgentRuntimes",
        "bedrock-agentcore:listApiKeyCredentialProviders",
        "bedrock-agentcore:listBrowserSessions",
        "bedrock-agentcore:listBrowsers",
        "bedrock-agentcore:listCodeInterpreterSessions",
        "bedrock-agentcore:listCodeInterpreters",
        "bedrock-agentcore:listEvaluators",
        "bedrock-agentcore:listEvents",
        "bedrock-agentcore:listGatewayTargets",
        "bedrock-agentcore:listGateways",
        "bedrock-agentcore:listMemories",
        "bedrock-agentcore:listMemoryExtractionJobs",
        "bedrock-agentcore:listMemoryRecords",
        "bedrock-agentcore:listOauth2CredentialProviders",
        "bedrock-agentcore:listOnlineEvaluationConfigs",
        "bedrock-agentcore:listPolicies",
        "bedrock-agentcore:listPolicyEngines",
        "bedrock-agentcore:listPolicyGenerationAssets",
        "bedrock-agentcore:listPolicyGenerations",
        "bedrock-agentcore:listSessions",
        "bedrock-agentcore:listWorkloadIdentities",
        "braket:getDevice",
        "braket:getJob",
        "braket:getQuantumTask",
        "braket:getServiceLinkedRoleStatus",
        "braket:getUserAgreementStatus",
        "braket:searchDevices",
```

```
        "braket:searchJobs",
        "braket:searchQuantumTasks",
        "braket:searchSpendingLimits",
        "budgets:viewBudget",
        "ce:getCostAndUsage",
        "ce:getCostAndUsageWithResources",
        "ce:getCostForecast",
        "ce:getDimensionValues",
        "ce:getReservationCoverage",
        "ce:getReservationPurchaseRecommendation",
        "ce:getReservationUtilization",
        "ce:getRightsizingRecommendation",
        "ce:getSavingsPlansCoverage",
        "ce:getSavingsPlansPurchaseRecommendation",
        "ce:getSavingsPlansUtilization",
        "ce:getSavingsPlansUtilizationDetails",
        "ce:getTags",
        "chime:describeAppInstance",
        "chime:getAttendee",
        "chime:getGlobalSettings",
        "chime:getMediaCapturePipeline",
        "chime:getMediaPipeline",
        "chime:getMeeting",
        "chime:getProxySession",
        "chime:getSipMediaApplication",
        "chime:getSipRule",
        "chime:getVoiceConnector",
        "chime:getVoiceConnectorGroup",
        "chime:getVoiceConnectorLoggingConfiguration",
        "chime:listAppInstances",
        "chime:listAttendees",
        "chime:listChannelBans",
        "chime:listChannels",
        "chime:listChannelsModeratedByAppInstanceUser",
        "chime:listMediaCapturePipelines",
        "chime:listMediaPipelines",
        "chime:listMeetings",
        "chime:listSipMediaApplications",
        "chime:listSipRules",
        "chime:listVoiceConnectorGroups",
        "chime:listVoiceConnectors",
        "cleanrooms:batchGetCollaborationAnalysisTemplate",
        "cleanrooms:batchGetSchema",
        "cleanrooms:getAnalysisTemplate",
```

```
        "cleanrooms:getCollaboration",
        "cleanrooms:getCollaborationAnalysisTemplate",
        "cleanrooms:getCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:getCollaborationPrivacyBudgetTemplate",
        "cleanrooms:getConfiguredTable",
        "cleanrooms:getConfiguredTableAnalysisRule",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getConfiguredAudienceModelAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getPrivacyBudgetTemplate",
        "cleanrooms:getSchema",
        "cleanrooms:getSchemaAnalysisRule",
        "cleanrooms:listAnalysisTemplates",
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:listCollaborationPrivacyBudgetTemplates",
        "cleanrooms:listCollaborationPrivacyBudgets",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredAudienceModelAssociations",
        "cleanrooms:listConfiguredTableAssociations",
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listPrivacyBudgetTemplates",
        "cleanrooms:listPrivacyBudgets",
        "cleanrooms:listProtectedQueries",
        "cleanrooms:listSchemas",
        "cleanrooms:previewPrivacyImpact",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describeEvents",
        "cloudformation:describePublisher",
        "cloudformation:describeStackDriftDetectionStatus",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResourceDrifts",
```

```
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getResource",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listResources",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeConnectionFunction",
        "cloudfront:describeFunction",
        "cloudfront:describeKeyValueStore",
        "cloudfront:getAnycastIpList",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getConnectionFunction",
        "cloudfront:getConnectionGroup",
        "cloudfront:getConnectionGroupByRoutingEndpoint",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getDistributionTenant",
        "cloudfront:getDistributionTenantByDomain",
        "cloudfront:getInvalidation",
        "cloudfront:getInvalidationForDistributionTenant",
        "cloudfront:getKeyGroup",
```

```
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getManagedCertificateDetails",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResourcePolicy",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:getTrustStore",
        "cloudfront:getVpcOrigin",
        "cloudfront:listAnycastIpLists",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listConnectionFunctions",
        "cloudfront:listConnectionGroups",
        "cloudfront:listConflictingAliases",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByAnycastIpListId",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByConnectionFunction",
        "cloudfront:listDistributionsByConnectionMode",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByTrustStore",
        "cloudfront:listDistributionsByVpcOriginId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listDistributionTenants",
        "cloudfront:listDistributionTenantsByCustomization",
        "cloudfront:listDomainConflicts",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listInvalidationsForDistributionTenant",
        "cloudfront:listKeyGroups",
        "cloudfront:listKeyValueStores",
```

```
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudfront:listTagsForResource",
        "cloudfront:listTrustStores",
        "cloudfront:listVpcOrigins",
        "cloudhsm:describeBackups",
        "cloudhsm:describeClusters",
        "cloudsearch:describeAnalysisSchemes",
        "cloudsearch:describeAvailabilityOptions",
        "cloudsearch:describeDomains",
        "cloudsearch:describeExpressions",
        "cloudsearch:describeIndexFields",
        "cloudsearch:describeScalingParameters",
        "cloudsearch:describeServiceAccessPolicies",
        "cloudsearch:describeSuggesters",
        "cloudsearch:listDomainNames",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:getInsightSelectors",
        "cloudtrail:getTrail",
        "cloudtrail:getTrailStatus",
        "cloudtrail:listEventDataStores",
        "cloudtrail:listPublicKeys",
        "cloudtrail:listTags",
        "cloudtrail:listTrails",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudWatch:getMetricWidgetImage",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetrics",
```

```
        "cloudwatch:listMetricStreams",
        "codeartifact:describeDomain",
        "codeartifact:describePackageVersion",
        "codeartifact:describeRepository",
        "codeartifact:getDomainPermissionsPolicy",
        "codeartifact:getRepositoryEndpoint",
        "codeartifact:getRepositoryPermissionsPolicy",
        "codeartifact:listDomains",
        "codeartifact:listPackages",
        "codeartifact:listPackageVersionAssets",
        "codeartifact:listPackageVersions",
        "codeartifact:listRepositories",
        "codeartifact:listRepositoriesInDomain",
        "codebuild:batchGetBuildBatches",
        "codebuild:batchGetBuilds",
        "codebuild:batchGetFleets",
        "codebuild:batchGetProjects",
        "codebuild:listBuildBatches",
        "codebuild:listBuildBatchesForProject",
        "codebuild:listBuilds",
        "codebuild:listBuildsForProject",
        "codebuild:listCuratedEnvironmentImages",
        "codebuild:listFleets",
        "codebuild:listProjects",
        "codebuild:listSourceCredentials",
        "codecommit:batchGetRepositories",
        "codecommit:getBranch",
        "codecommit:getRepository",
        "codecommit:getRepositoryTriggers",
        "codecommit:listBranches",
        "codecommit:listRepositories",
        "codeconnections:getConnection",
        "codeconnections:getHost",
        "codeconnections:getRepositoryLink",
        "codeconnections:getRepositorySyncStatus",
        "codeconnections:getResourceSyncStatus",
        "codeconnections:getSyncBlockerSummary",
        "codeconnections:getSyncConfiguration",
        "codeconnections:listConnections",
        "codeconnections:listHosts",
        "codeconnections:listRepositoryLinks",
        "codeconnections:listRepositorySyncDefinitions",
        "codeconnections:listSyncConfigurations",
        "codedeploy:batchGetApplicationRevisions",
```

```
        "codedeploy:batchGetApplications",
        "codedeploy:batchGetDeploymentGroups",
        "codedeploy:batchGetDeploymentInstances",
        "codedeploy:batchGetDeployments",
        "codedeploy:batchGetDeploymentTargets",
        "codedeploy:batchGetOnPremisesInstances",
        "codedeploy:getApplication",
        "codedeploy:getApplicationRevision",
        "codedeploy:getDeployment",
        "codedeploy:getDeploymentConfig",
        "codedeploy:getDeploymentGroup",
        "codedeploy:getDeploymentInstance",
        "codedeploy:getDeploymentTarget",
        "codedeploy:getOnPremisesInstance",
        "codedeploy:listApplicationRevisions",
        "codedeploy:listApplications",
        "codedeploy:listDeploymentConfigs",
        "codedeploy:listDeploymentGroups",
        "codedeploy:listDeploymentInstances",
        "codedeploy:listDeployments",
        "codedeploy:listDeploymentTargets",
        "codedeploy:listGitHubAccountTokenNames",
        "codedeploy:listOnPremisesInstances",
        "codepipeline:getJobDetails",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineExecution",
        "codepipeline:getPipelineState",
        "codepipeline:listActionExecutions",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "codepipeline:listRuleExecutions",
        "codepipeline:listWebhooks",
        "codestar-connections:getConnection",
        "codestar-connections:getHost",
        "codestar-connections:listConnections",
        "codestar-connections:listHosts",
        "codestar:describeProject",
        "codestar:listProjects",
        "codestar:listResources",
        "codestar:listTeamMembers",
        "codestar:listUserProfiles",
        "cognito-identity:describeIdentity",
        "cognito-identity:describeIdentityPool",
```

```
        "cognito-identity:getIdentityPoolAnalytics",
        "cognito-identity:getIdentityPoolDailyAnalytics",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:getIdentityProviderDailyAnalytics",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-identity:lookupDeveloperIdentity",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeManagedLoginBranding",
        "cognito-idp:describeManagedLoginBrandingByClient",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getCSVHeader",
        "cognito-idp:getGroup",
        "cognito-idp:getLogDeliveryConfiguration",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:getWebACLForResource",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listResourcesForWebACL",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "comprehend:describeDocumentClassificationJob",
        "comprehend:describeDocumentClassifier",
        "comprehend:describeDominantLanguageDetectionJob",
        "comprehend:describeEndpoint",
        "comprehend:describeEntitiesDetectionJob",
        "comprehend:describeEntityRecognizer",
        "comprehend:describeEventsDetectionJob",
        "comprehend:describeFlywheel",
```

```
        "comprehend:describeFlywheelIteration",
        "comprehend:describeKeyPhrasesDetectionJob",
        "comprehend:describePiiEntitiesDetectionJob",
        "comprehend:describeSentimentDetectionJob",
        "comprehend:describeTargetedSentimentDetectionJob",
        "comprehend:describeTopicsDetectionJob",
        "comprehend:listDocumentClassificationJobs",
        "comprehend:listDocumentClassifiers",
        "comprehend:listDominantLanguageDetectionJobs",
        "comprehend:listEndpoints",
        "comprehend:listEntitiesDetectionJobs",
        "comprehend:listEntityRecognizers",
        "comprehend:listEventsDetectionJobs",
        "comprehend:listFlywheelIterationHistory",
        "comprehend:listFlywheels",
        "comprehend:listKeyPhrasesDetectionJobs",
        "comprehend:listPiiEntitiesDetectionJobs",
        "comprehend:listSentimentDetectionJobs",
        "comprehend:listTargetedSentimentDetectionJobs",
        "comprehend:listTopicsDetectionJobs",
        "compute-optimizer:getAutoScalingGroupRecommendations",
        "compute-optimizer:getEBSVolumeRecommendations",
        "compute-optimizer:getEC2InstanceRecommendations",
        "compute-optimizer:getEC2RecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getEnrollmentStatus",
        "compute-optimizer:getIdleRecommendations",
        "compute-optimizer:getRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:getRDSDatabaseRecommendations",
        "compute-optimizer:getRecommendationSummaries",
        "config:batchGetAggregateResourceConfig",
        "config:batchGetResourceConfig",
        "config:describeAggregateComplianceByConfigRules",
        "config:describeAggregationAuthorizations",
        "config:describeComplianceByConfigRule",
        "config:describeComplianceByResource",
        "config:describeConfigRuleEvaluationStatus",
        "config:describeConfigRules",
        "config:describeConfigurationAggregators",
        "config:describeConfigurationAggregatorSourcesStatus",
        "config:describeConfigurationRecorders",
        "config:describeConfigurationRecorderStatus",
        "config:describeConformancePackCompliance",
```

```
        "config:describeConformancePacks",
        "config:describeConformancePackStatus",
        "config:describeDeliveryChannels",
        "config:describeDeliveryChannelStatus",
        "config:describeOrganizationConfigRules",
        "config:describeOrganizationConfigRuleStatuses",
        "config:describeOrganizationConformancePacks",
        "config:describeOrganizationConformancePackStatuses",
        "config:describePendingAggregationRequests",
        "config:describeRemediationConfigurations",
        "config:describeRemediationExceptions",
        "config:describeRemediationExecutionStatus",
        "config:describeRetentionConfigurations",
        "config:getAggregateComplianceDetailsByConfigRule",
        "config:getAggregateConfigRuleComplianceSummary",
        "config:getAggregateDiscoveredResourceCounts",
        "config:getAggregateResourceConfig",
        "config:getComplianceDetailsByConfigRule",
        "config:getComplianceDetailsByResource",
        "config:getComplianceSummaryByConfigRule",
        "config:getComplianceSummaryByResourceType",
        "config:getConformancePackComplianceDetails",
        "config:getConformancePackComplianceSummary",
        "config:getDiscoveredResourceCounts",
        "config:getOrganizationConfigRuleDetailedStatus",
        "config:getOrganizationConformancePackDetailedStatus",
        "config:getResourceConfigHistory",
        "config:listAggregateDiscoveredResources",
        "config:listDiscoveredResources",
        "config:listTagsForResource",
        "config:selectAggregateResourceConfig",
        "config:selectResourceConfig",
        "connect:batchGetFlowAssociation",
        "connect:describeContact",
        "connect:describeContactFlow",
        "connect:describeInstance",
        "connect:describeInstanceAttribute",
        "connect:describePhoneNumber",
        "connect:describeQueue",
        "connect:describeQuickConnect",
        "connect:describeRoutingProfile",
        "connect:describeUser",
        "connect:describeUserHierarchyStructure",
        "connect:getCurrentMetricData",
```

```
        "connect:getMetricData",
        "connect:getMetricDataV2",
        "connect:listContactEvaluations",
        "connect:listEvaluationForms",
        "connect:listEvaluationFormVersions",
        "connect:listInstanceAttributes",
        "connect:listPhoneNumbersV2",
        "connect:listQueueQuickConnects",
        "connect:listQueues",
        "connect:listQuickConnects",
        "connect:listRoutingProfileQueues",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listSecurityProfilePermissions",
        "connect:listUsers",
        "connect:listViews",
        "connect:listViewVersions",
        "connect:searchQueues",
        "connect:searchRoutingProfiles",
        "connect:searchUsers",
        "connect-campaigns:describeCampaign",
        "controlcatalog:getControl",
        "controltower:describeAccountFactoryConfig",
        "controltower:describeCoreService",
        "controltower:describeGuardrail",
        "controltower:describeGuardrailForTarget",
        "controltower:describeManagedAccount",
        "controltower:describeSingleSignOn",
        "controltower:getAvailableUpdates",
        "controltower:getBaselineOperation",
        "controltower:getControlOperation",
        "controltower:getEnabledBaseline",
        "controltower:getEnabledControl",
        "controltower:getHomeRegion",
        "controltower:getLandingZone",
        "controltower:getLandingZoneStatus",
        "controltower:listBaselines",
        "controltower:listDirectoryGroups",
        "controltower:listEnabledControls",
        "controltower:listEnabledBaselines",
        "controltower:listGuardrailsForTarget",
        "controltower:listGuardrailViolations",
        "controltower:listLandingZones",
        "controltower:listManagedAccounts",
```

```
        "controltower:listManagedAccountsForGuardrail",
        "controltower:listManagedAccountsForParent",
        "controltower:listManagedOrganizationalUnits",
        "controltower:listManagedOrganizationalUnitsForGuardrail",
        "cost-optimization-hub:getPreferences",
        "cost-optimization-hub:getRecommendation",
        "cost-optimization-hub:listEnrollmentStatuses",
        "cost-optimization-hub:listRecommendations",
        "cost-optimization-hub:listRecommendationSummaries",
        "databrew:describeDataset",
        "databrew:describeJob",
        "databrew:describeProject",
        "databrew:describeRecipe",
        "databrew:listDatasets",
        "databrew:listJobRuns",
        "databrew:listJobs",
        "databrew:listProjects",
        "databrew:listRecipes",
        "databrew:listRecipeVersions",
        "databrew:listTagsForResource",
        "datapipeline:describeObjects",
        "datapipeline:describePipelines",
        "datapipeline:getPipelineDefinition",
        "datapipeline:listPipelines",
        "datapipeline:queryObjects",
        "datasync:describeAgent",
        "datasync:describeLocationAzureBlob",
        "datasync:describeLocationEfs",
        "datasync:describeLocationFsxLustre",
        "datasync:describeLocationFsxOntap",
        "datasync:describeLocationFsxOpenZfs",
        "datasync:describeLocationFsxWindows",
        "datasync:describeLocationHdfs",
        "datasync:describeLocationNfs",
        "datasync:describeLocationObjectStorage",
        "datasync:describeLocationS3",
        "datasync:describeLocationSmb",
        "datasync:describeTask",
        "datasync:describeTaskExecution",
        "datasync:listAgents",
        "datasync:listLocations",
        "datasync:listTaskExecutions",
        "datasync:listTasks",
        "datazone:getAsset",
```

```
        "datazone:getAssetType",
        "datazone:getDataSource",
        "datazone:getDataSourceRun",
        "datazone:getDomain",
        "datazone:getEnvironment",
        "datazone:getEnvironmentBlueprint",
        "datazone:getEnvironmentBlueprintConfiguration",
        "datazone:getEnvironmentProfile",
        "datazone:getFormType",
        "datazone:getGlossary",
        "datazone:getGlossaryTerm",
        "datazone:getGroupProfile",
        "datazone:getListing",
        "datazone:getMetadataGenerationRun",
        "datazone:getProject",
        "datazone:getSubscription",
        "datazone:getSubscriptionGrant",
        "datazone:getSubscriptionRequestDetails",
        "datazone:getSubscriptionTarget",
        "datazone:getUserProfile",
        "datazone:listAssetRevisions",
        "datazone:listDataSourceRunActivities",
        "datazone:listDataSourceRuns",
        "datazone:listDataSources",
        "datazone:listDomains",
        "datazone:listEnvironmentBlueprintConfigurations",
        "datazone:listEnvironmentBlueprints",
        "datazone:listEnvironmentProfiles",
        "datazone:listEnvironments",
        "datazone:listMetadataGenerationRuns",
        "datazone:listProjectMemberships",
        "datazone:listProjects",
        "datazone:listSubscriptionGrants",
        "datazone:listSubscriptionRequests",
        "datazone:listSubscriptions",
        "datazone:listSubscriptionTargets",
        "datazone:searchGroupProfiles",
        "datazone:searchUserProfiles",
        "dax:describeClusters",
        "dax:describeDefaultParameters",
        "dax:describeEvents",
        "dax:describeParameterGroups",
        "dax:describeParameters",
        "dax:describeSubnetGroups",
```

```
        "deadline:listAvailableMeteredProducts",
        "deadline:listBudgets",
        "deadline:listFarmMembers",
        "deadline:listFarms",
        "deadline:listFleetMembers",
        "deadline:listFleets",
        "deadline:listJobMembers",
        "deadline:listJobs",
        "deadline:listLicenseEndpoints",
        "deadline:listMeteredProducts",
        "deadline:listMonitors",
        "deadline:listQueueEnvironments",
        "deadline:listQueueFleetAssociations",
        "deadline:listQueueMembers",
        "deadline:listQueues",
        "deadline:listStorageProfiles",
        "deadline:listWorkers",
        "detective:getMembers",
        "detective:listGraphs",
        "detective:listInvitations",
        "detective:listMembers",
        "devicefarm:getAccountSettings",
        "devicefarm:getDevice",
        "devicefarm:getDevicePool",
        "devicefarm:getDevicePoolCompatibility",
        "devicefarm:getJob",
        "devicefarm:getOfferingStatus",
        "devicefarm:getProject",
        "devicefarm:getRemoteAccessSession",
        "devicefarm:getRun",
        "devicefarm:getSuite",
        "devicefarm:getTest",
        "devicefarm:getTestGridProject",
        "devicefarm:getTestGridSession",
        "devicefarm:getUpload",
        "devicefarm:getVPCEConfiguration",
        "devicefarm:listArtifacts",
        "devicefarm:listDevicePools",
        "devicefarm:listDevices",
        "devicefarm:listJobs",
        "devicefarm:listNetworkProfiles",
        "devicefarm:listOfferingPromotions",
        "devicefarm:listOfferingTransactions",
        "devicefarm:listProjects",
```

```
        "devicefarm:listRemoteAccessSessions",
        "devicefarm:listRuns",
        "devicefarm:listSamples",
        "devicefarm:listSuites",
        "devicefarm:listTestGridProjects",
        "devicefarm:listTestGridSessionActions",
        "devicefarm:listTestGridSessionArtifacts",
        "devicefarm:listTestGridSessions",
        "devicefarm:listTests",
        "devicefarm:listUniqueProblems",
        "devicefarm:listUploads",
        "devicefarm:listVPCEConfigurations",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "directconnect:listVirtualInterfaceTestHistory",
        "dlm:getLifecyclePolicies",
        "dlm:getLifecyclePolicy",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpoints",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEventCategories",
        "dms:describeEvents",
        "dms:describeEventSubscriptions",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
```

```
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstances",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "docdb-elastic:getCluster",
        "docdb-elastic:getClusterSnapshot",
        "docdb-elastic:listClusters",
        "docdb-elastic:listClusterSnapshots",
        "drs:describeJobLogItems",
        "drs:describeJobs",
        "drs:describeLaunchConfigurationTemplates",
        "drs:describeRecoveryInstances",
        "drs:describeRecoverySnapshots",
        "drs:describeReplicationConfigurationTemplates",
        "drs:describeSourceNetworks",
        "drs:describeSourceServers",
        "drs:getLaunchConfiguration",
        "drs:getReplicationConfiguration",
        "drs:listExtensibleSourceServers",
        "drs:listLaunchActions",
        "drs:listStagingAccounts",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeHybridADUpdate",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
```

```
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dsql:getCluster",
        "dsql:getVpcEndpointServiceName",
        "dsql:listClusters",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeGlobalTableSettings",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTableReplicaAutoScaling",
        "dynamodb:describeTimeToLive",
        "dynamodb:getResourcePolicy",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ebs:listChangedBlocks",
        "ebs:listSnapshotBlocks",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityBlockOfferings",
        "ec2:describeCapacityManagerDataExports",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
```

```
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdentityIdFormat",
        "ec2:describeIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceConnectEndpoints",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstances",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInternetGateways",
        "ec2:describeIpamByoasn",
        "ec2:describeIpamExternalResourceVerificationTokens",
        "ec2:describeIpamPools",
        "ec2:describeIpamResourceDiscoveries",
        "ec2:describeIpamResourceDiscoveryAssociations",
```

```
        "ec2:describeIpams",
        "ec2:describeIpamScopes",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplates",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGateways",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInsightsAccessScopeAnalyses",
        "ec2:describeNetworkInsightsAccessScopes",
        "ec2:describeNetworkInsightsAnalyses",
        "ec2:describeNetworkInsightsPaths",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describeOutpostLags",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReplaceRootVolumeTasks",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteServerEndpoints",
        "ec2:describeRouteServerPeers",
        "ec2:describeRouteServers",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeServiceLinkVirtualInterfaces",
        "ec2:describeSnapshotAttribute",
```

```
        "ec2:describeSnapshots",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilterRules",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayConnects",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessInstanceWebAclAssociations",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcBlockPublicAccessExclusions",
        "ec2:describeVpcBlockPublicAccessOptions",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointAssociations",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
```

```
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcEncryptionControls",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedEnclaveCertificateIamRoles",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityManagerAttributes",
        "ec2:getCapacityManagerMetricData",
        "ec2:getCapacityManagerMetricDimensions",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getImageBlockPublicAccessState",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamDiscoveredAccounts",
        "ec2:getIpamDiscoveredPublicAddresses",
        "ec2:getIpamDiscoveredResourceCidrs",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getNetworkInsightsAccessScopeContent",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getRouteServerAssociations",
        "ec2:getRouteServerPropagations",
        "ec2:getRouteServerRoutingDatabase",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getSubnetCidrReservations",
        "ec2:getTransitGatewayAttachmentPropagations",
```

```
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPolicyTableAssociations",
        "ec2:getTransitGatewayPolicyTableEntries",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getTransitGatewayRouteTableAssociations",
        "ec2:getTransitGatewayRouteTablePropagations",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:getVpcResourcesBlockingEncryptionEnforcement",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecr-public:describeImages",
        "ecr-public:describeImageTags",
        "ecr-public:describeRegistries",
        "ecr-public:describeRepositories",
        "ecr-public:getRegistryCatalogData",
        "ecr-public:getRepositoryCatalogData",
        "ecr-public:getRepositoryPolicy",
        "ecr-public:listTagsForResource",
        "ecr:batchCheckLayerAvailability",
        "ecr:batchGetImage",
        "ecr:batchGetRepositoryScanningConfiguration",
        "ecr:describeImageReplicationStatus",
        "ecr:describeImages",
        "ecr:describeImageScanFindings",
        "ecr:describeImageSigningStatus",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:describeRepositoryCreationTemplates",
        "ecr:getAccountSetting",
        "ecr:getAuthorizationToken",
        "ecr:getDownloadUrlForLayer",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:getSigningConfiguration",
        "ecr:listImages",
        "ecr:listPullTimeUpdateExclusions",
```

```
        "ecr:listTagsForResource",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeExpressGatewayService",
        "ecs:describeServiceDeployments",
        "ecs:describeServiceRevisions",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServiceDeployments",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup2",
      "Effect" : "Allow",
      "Action" : [
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCapability",
        "eks:describeCluster",
        "eks:describeClusterVersions",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeInsight",
        "eks:describeNodegroup",
```

```
        "eks:describePodIdentityAssociation",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listInsights",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
```

```
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:listTagsForResource",
        "elasticbeanstalk:describeConfigurationSettings",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeBackupPolicy",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeReplicationConfigurations",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describePersistentAppUI",
        "elasticmapreduce:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
```

```
        "elasticmapreduce:getAutoTerminationPolicy",
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
        "elasticmapreduce:listStudioSessionMappings",
        "elasticmapreduce:listSupportedInstanceTypes",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "emr-serverless:listJobRunAttempts",
        "emr-serverless:listJobRuns",
        "entityresolution:getIdMappingJob",
        "entityresolution:getIdMappingWorkflow",
        "entityresolution:getMatchingJob",
        "entityresolution:getMatchingWorkflow",
        "entityresolution:getProviderService",
        "entityresolution:getSchemaMapping",
        "entityresolution:listIdMappingJobs",
        "entityresolution:listIdMappingWorkflows",
        "entityresolution:listMatchingJobs",
        "entityresolution:listMatchingWorkflows",
        "entityresolution:listProviderServices",
        "entityresolution:listSchemaMappings",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
```

```
        "es:describeDomainConfig",
        "es:describeDomainHealth",
        "es:describeDomainNodes",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:getDomainMaintenanceStatus",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeInsightDetails",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainMaintenances",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listInsights",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
```

```
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "evs:getEnvironment",
        "evs:getVersions",
        "evs:listEnvironmentHosts",
        "evs:listEnvironments",
        "evs:listEnvironmentVlans",
        "evs:listTagsForResource",
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fis:getAction",
        "fis:getExperiment",
        "fis:getExperimentTargetAccountConfiguration",
        "fis:getExperimentTemplate",
        "fis:getSafetyLever",
        "fis:getTargetAccountConfiguration",
        "fis:listActions",
        "fis:listExperimentResolvedTargets",
        "fis:listExperimentTargetAccountConfigurations",
        "fis:listExperiments",
        "fis:listExperimentTemplates",
        "fis:listTargetAccountConfigurations",
        "fms:getAdminAccount",
        "fms:getAdminScope",
        "fms:getAppsList",
        "fms:getComplianceDetail",
        "fms:getNotificationChannel",
        "fms:getProtocolsList",
        "fms:getPolicy",
        "fms:getProtectionStatus",
        "fms:getResourceSet",
        "fms:getThirdPartyFirewallAssociationStatus",
        "fms:getViolationDetails",
        "fms:listAdminAccountsForOrganization",
        "fms:listAdminsManagingAccount",
```

```
        "fms:listAppsLists",
        "fms:listComplianceStatus",
        "fms:listDiscoveredResources",
        "fms:listMemberAccounts",
        "fms:listProtocolsLists",
        "fms:listPolicies",
        "fms:listResourceSetResources",
        "fms:listResourceSets",
        "fms:listThirdPartyFirewallFirewallPolicies",
        "forecast:describeDataset",
        "forecast:describeDatasetGroup",
        "forecast:describeDatasetImportJob",
        "forecast:describeForecast",
        "forecast:describeForecastExportJob",
        "forecast:describePredictor",
        "forecast:getAccuracyMetrics",
        "forecast:listDatasetGroups",
        "forecast:listDatasetImportJobs",
        "forecast:listDatasets",
        "forecast:listForecastExportJobs",
        "forecast:listForecasts",
        "forecast:listPredictors",
        "freetier:getFreeTierUsage",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeS3AccessPointAttachments",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "gamelift:describeAlias",
        "gamelift:describeBuild",
        "gamelift:describeEC2InstanceLimits",
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
```

```
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
        "gamelift:resolveAlias",
        "geo:calculateRoute",
        "geo:calculateRouteMatrix",
        "geo:describeMap",
        "geo:describePlaceIndex",
        "geo:describeRouteCalculator",
        "geo:describeTracker",
        "geo:getMapGlyphs",
        "geo:getMapSprites",
        "geo:getMapStyleDescriptor",
        "geo:getMapTile",
        "geo:getPlace",
        "geo:listGeofenceCollections",
        "geo:listMaps",
        "geo:listPlaceIndexes",
        "geo:listRouteCalculators",
        "geo:listTrackerConsumers",
        "geo:searchPlaceIndexForPosition",
        "geo:searchPlaceIndexForSuggestions",
        "geo:searchPlaceIndexForText",
        "geo-maps:getStaticMap",
        "geo-maps:getTile",
        "geo-places:autocomplete",
        "geo-places:geocode",
```

```
        "geo-places:getPlace",
        "geo-places:reverseGeocode",
        "geo-places:searchNearby",
        "geo-places:searchText",
        "geo-places:suggest",
        "geo-routes:calculateIsolines",
        "geo-routes:calculateRouteMatrix",
        "geo-routes:calculateRoutes",
        "geo-routes:optimizeWaypoints",
        "geo-routes:snapToRoads",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeCrossAccountAttachment",
        "globalaccelerator:describeCustomRoutingAccelerator",
        "globalaccelerator:describeCustomRoutingAcceleratorAttributes",
        "globalaccelerator:describeCustomRoutingEndpointGroup",
        "globalaccelerator:describeCustomRoutingListener",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listByoipCidrs",
        "globalaccelerator:listCrossAccountAttachments",
        "globalaccelerator:listCrossAccountResourceAccounts",
        "globalaccelerator:listCrossAccountResources",
        "globalaccelerator:listCustomRoutingAccelerators",
        "globalaccelerator:listCustomRoutingEndpointGroups",
        "globalaccelerator:listCustomRoutingListeners",
        "globalaccelerator:listCustomRoutingPortMappings",
        "globalaccelerator:listCustomRoutingPortMappingsByDestination",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
```

```
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:batchGetTableOptimizer",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalog",
        "glue:getCatalogImportStatus",
        "glue:getCatalogs",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getColumnStatisticsTaskRun",
        "glue:getColumnStatisticsTaskRuns",
        "glue:getCompletion",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataCatalogEncryptionSettings",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobBookmark",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
```

```
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSecurityConfiguration",
        "glue:getSecurityConfigurations",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableOptimizer",
        "glue:getTableVersion",
        "glue:getTables",
        "glue:getTableVersions",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listColumnStatisticsTaskRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
        "glue:listTableOptimizerRuns",
        "glue:listTriggers",
        "glue:querySchemaVersionMetadata",
        "glue:startCompletion",
        "grafana:describeWorkspace",
        "grafana:describeWorkspaceAuthentication",
```

```
        "grafana:listPermissions",
        "grafana:listVersions",
        "grafana:listWorkspaces",
        "greengrass:describeComponent",
        "greengrass:getComponent",
        "greengrass:getConnectivityInfo",
        "greengrass:getCoreDefinition",
        "greengrass:getCoreDefinitionVersion",
        "greengrass:getCoreDevice",
        "greengrass:getDeployment",
        "greengrass:getDeploymentStatus",
        "greengrass:getDeviceDefinition",
        "greengrass:getDeviceDefinitionVersion",
        "greengrass:getFunctionDefinition",
        "greengrass:getFunctionDefinitionVersion",
        "greengrass:getGroup",
        "greengrass:getGroupCertificateAuthority",
        "greengrass:getGroupVersion",
        "greengrass:getLoggerDefinition",
        "greengrass:getLoggerDefinitionVersion",
        "greengrass:getResourceDefinitionVersion",
        "greengrass:getServiceRoleForAccount",
        "greengrass:getSubscriptionDefinition",
        "greengrass:getSubscriptionDefinitionVersion",
        "greengrass:listClientDevicesAssociatedWithCoreDevice",
        "greengrass:listComponents",
        "greengrass:listComponentVersions",
        "greengrass:listCoreDefinitions",
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listCoreDevices",
        "greengrass:listDeployments",
        "greengrass:listEffectiveDeployments",
        "greengrass:listInstalledComponents",
        "greengrass:listDeviceDefinitions",
        "greengrass:listDeviceDefinitionVersions",
        "greengrass:listFunctionDefinitions",
        "greengrass:listFunctionDefinitionVersions",
        "greengrass:listGroups",
        "greengrass:listGroupVersions",
        "greengrass:listLoggerDefinitions",
        "greengrass:listLoggerDefinitionVersions",
        "greengrass:listResourceDefinitions",
        "greengrass:listResourceDefinitionVersions",
        "greengrass:listSubscriptionDefinitions",
```

```
        "greengrass:listSubscriptionDefinitionVersions",
        "guardduty:describeMalwareScans",
        "guardduty:describePublishingDestination",
        "guardduty:getCoverageStatistics",
        "guardduty:getDetector",
        "guardduty:getFilter",
        "guardduty:getFindings",
        "guardduty:getFindingsStatistics",
        "guardduty:getInvitationsCount",
        "guardduty:getIPSet",
        "guardduty:getMalwareScanSettings",
        "guardduty:getMasterAccount",
        "guardduty:getMemberDetectors",
        "guardduty:getMembers",
        "guardduty:getOrganizationStatistics",
        "guardduty:getRemainingFreeTrialDays",
        "guardduty:getThreatIntelSet",
        "guardduty:listCoverage",
        "guardduty:listDetectors",
        "guardduty:listFilters",
        "guardduty:listFindings",
        "guardduty:listInvitations",
        "guardduty:listIPSets",
        "guardduty:listMembers",
        "guardduty:listThreatIntelSets",
        "health:describeAffectedAccountsForOrganization",
        "health:describeAffectedEntities",
        "health:describeAffectedEntitiesForOrganization",
        "health:describeEntityAggregates",
        "health:describeEntityAggregatesForOrganization",
        "health:describeEventAggregates",
        "health:describeEventDetails",
        "health:describeEventDetailsForOrganization",
        "health:describeEvents",
        "health:describeEventsForOrganization",
        "health:describeEventTypes",
        "health:describeHealthServiceStatusForOrganization",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
```

```
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getMFADevice",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getSSHPublicKey",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listServerCertificates",
        "iam:listServiceSpecificCredentials",
        "iam:listSigningCertificates",
        "iam:listSSHPublicKeys",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "identitystore:describeGroup",
```

```
        "identitystore:describeGroupMembership",
        "identitystore:describeUser",
        "identitystore:getGroupId",
        "identitystore:getGroupMembershipId",
        "identitystore:getUserId",
        "identitystore:isMemberInGroups",
        "identitystore:listGroupMemberships",
        "identitystore:listGroupMembershipsForMember",
        "identitystore:listGroups",
        "identitystore:listUsers",
        "imagebuilder:getComponent",
        "imagebuilder:getComponentPolicy",
        "imagebuilder:getContainerRecipe",
        "imagebuilder:getContainerRecipePolicy",
        "imagebuilder:getDistributionConfiguration",
        "imagebuilder:getImage",
        "imagebuilder:getImagePipeline",
        "imagebuilder:getImagePolicy",
        "imagebuilder:getImageRecipe",
        "imagebuilder:getImageRecipePolicy",
        "imagebuilder:getInfrastructureConfiguration",
        "imagebuilder:getLifecycleExecution",
        "imagebuilder:getLifecyclePolicy",
        "imagebuilder:getWorkflow",
        "imagebuilder:getWorkflowExecution",
        "imagebuilder:getWorkflowStepExecution",
        "imagebuilder:listComponentBuildVersions",
        "imagebuilder:listComponents",
        "imagebuilder:listContainerRecipes",
        "imagebuilder:listDistributionConfigurations",
        "imagebuilder:listImageBuildVersions",
        "imagebuilder:listImagePipelineImages",
        "imagebuilder:listImagePipelines",
        "imagebuilder:listImageRecipes",
        "imagebuilder:listImages",
        "imagebuilder:listImageScanFindingAggregations",
        "imagebuilder:listInfrastructureConfigurations",
        "imagebuilder:listLifecycleExecutionResources",
        "imagebuilder:listLifecycleExecutions",
        "imagebuilder:listLifecyclePolicies",
        "imagebuilder:listTagsForResource",
        "imagebuilder:listWorkflowBuildVersions",
        "imagebuilder:listWorkflowExecutions",
        "imagebuilder:listWorkflows",
```

```
        "imagebuilder:listWaitingWorkflowSteps",
        "imagebuilder:listWorkflowStepExecutions",
        "inspector-scan:scanSbom",
        "inspector:describeAssessmentRuns",
        "inspector:describeAssessmentTargets",
        "inspector:describeAssessmentTemplates",
        "inspector:describeCrossAccountAccessRole",
        "inspector:describeResourceGroups",
        "inspector:describeRulesPackages",
        "inspector:getTelemetryMetadata",
        "inspector:listAssessmentRunAgents",
        "inspector:listAssessmentRuns",
        "inspector:listAssessmentTargets",
        "inspector:listAssessmentTemplates",
        "inspector:listEventSubscriptions",
        "inspector:listRulesPackages",
        "inspector:listTagsForResource",
        "inspector2:batchGetAccountStatus",
        "inspector2:batchGetFreeTrialInfo",
        "inspector2:describeOrganizationConfiguration",
        "inspector2:getConfiguration",
        "inspector2:getDelegatedAdminAccount",
        "inspector2:getEc2DeepInspectionConfiguration",
        "inspector2:getMember",
        "inspector2:getSbomExport",
        "inspector2:listCisScanConfigurations",
        "inspector2:listCisScanResultsAggregatedByChecks",
        "inspector2:listCisScanResultsAggregatedByTargetResource",
        "inspector2:listCisScans",
        "inspector2:listCoverage",
        "inspector2:listDelegatedAdminAccounts",
        "inspector2:listFilters",
        "inspector2:listFindings",
        "inspector2:listMembers",
        "inspector2:listUsageTotals",
        "internetmonitor:getHealthEvent",
        "internetmonitor:getMonitor",
        "internetmonitor:listHealthEvents",
        "internetmonitor:listMonitors",
        "invoicing:batchGetInvoiceProfile",
        "invoicing:listInvoiceSummaries",
        "invoicing:listInvoiceUnits",
        "iot:describeAuthorizer",
        "iot:describeCACertificate",
```

```
        "iot:describeCertificate",
        "iot:describeDefaultAuthorizer",
        "iot:describeDomainConfiguration",
        "iot:describeEndpoint",
        "iot:describeIndex",
        "iot:describeJobExecution",
        "iot:describeThing",
        "iot:describeThingGroup",
        "iot:describeTunnel",
        "iot:getEffectivePolicies",
        "iot:getIndexingConfiguration",
        "iot:getLoggingOptions",
        "iot:getPolicy",
        "iot:getPolicyVersion",
        "iot:getTopicRule",
        "iot:getV2LoggingOptions",
        "iot:listAttachedPolicies",
        "iot:listAuthorizers",
        "iot:listCACertificates",
        "iot:listCertificates",
        "iot:listCertificatesByCA",
        "iot:listCommandExecutions",
        "iot:listCommands",
        "iot:listDomainConfigurations",
        "iot:listJobExecutionsForJob",
        "iot:listJobExecutionsForThing",
        "iot:listJobs",
        "iot:listNamedShadowsForThing",
        "iot:listOutgoingCertificates",
        "iot:listPackages",
        "iot:listPackageVersions",
        "iot:listPolicies",
        "iot:listPolicyPrincipals",
        "iot:listPolicyVersions",
        "iot:listPrincipalPolicies",
        "iot:listPrincipalThings",
        "iot:listRoleAliases",
        "iot:listTargetsForPolicy",
        "iot:listThingGroups",
        "iot:listThingGroupsForThing",
        "iot:listThingPrincipals",
        "iot:listThingRegistrationTasks",
        "iot:listThings",
        "iot:listThingsInThingGroup",
```

```
        "iot:listThingTypes",
        "iot:listTopicRules",
        "iot:listTunnels",
        "iot:listV2LoggingLevels",
        "iotevents:describeDetector",
        "iotevents:describeDetectorModel",
        "iotevents:describeInput",
        "iotevents:describeLoggingOptions",
        "iotevents:listDetectorModels",
        "iotevents:listDetectorModelVersions",
        "iotevents:listDetectors",
        "iotevents:listInputs",
        "iotfleetwise:getCampaign",
        "iotfleetwise:getDecoderManifest",
        "iotfleetwise:getEncryptionConfiguration",
        "iotfleetwise:getFleet",
        "iotfleetwise:getLoggingOptions",
        "iotfleetwise:getModelManifest",
        "iotfleetwise:getRegisterAccountStatus",
        "iotfleetwise:getSignalCatalog",
        "iotfleetwise:getStateTemplate",
        "iotfleetwise:getVehicle",
        "iotfleetwise:getVehicleStatus",
        "iotfleetwise:listCampaigns",
        "iotfleetwise:listDecoderManifestNetworkInterfaces",
        "iotfleetwise:listDecoderManifests",
        "iotfleetwise:listDecoderManifestSignals",
        "iotfleetwise:listFleets",
        "iotfleetwise:listFleetsForVehicle",
        "iotfleetwise:listModelManifestNodes",
        "iotfleetwise:listModelManifests",
        "iotfleetwise:listSignalCatalogNodes",
        "iotfleetwise:listSignalCatalogs",
        "iotfleetwise:listStateTemplates",
        "iotfleetwise:listVehicles",
        "iotfleetwise:listVehiclesInFleet",
        "iotsitewise:describeAccessPolicy",
        "iotsitewise:describeAsset",
        "iotsitewise:describeAssetModel",
        "iotsitewise:describeAssetProperty",
        "iotsitewise:describeDashboard",
        "iotsitewise:describeGateway",
        "iotsitewise:describeGatewayCapabilityConfiguration",
        "iotsitewise:describeLoggingOptions",
```

```
        "iotsitewise:describePortal",
        "iotsitewise:describeProject",
        "iotsitewise:listAccessPolicies",
        "iotsitewise:listAssetModels",
        "iotsitewise:listAssets",
        "iotsitewise:listAssociatedAssets",
        "iotsitewise:listDashboards",
        "iotsitewise:listGateways",
        "iotsitewise:listPortals",
        "iotsitewise:listProjectAssets",
        "iotsitewise:listProjects",
        "iottwinmaker:getComponentType",
        "iottwinmaker:getEntity",
        "iottwinmaker:getPricingPlan",
        "iottwinmaker:getScene",
        "iottwinmaker:getSyncJob",
        "iottwinmaker:getWorkspace",
        "iottwinmaker:listComponentTypes",
        "iottwinmaker:listEntities",
        "iottwinmaker:listScenes",
        "iottwinmaker:listSyncJobs",
        "iottwinmaker:listSyncResources",
        "iottwinmaker:listWorkspaces",
        "iotwireless:getDestination",
        "iotwireless:getDeviceProfile",
        "iotwireless:getPartnerAccount",
        "iotwireless:getServiceEndpoint",
        "iotwireless:getServiceProfile",
        "iotwireless:getWirelessDevice",
        "iotwireless:getWirelessDeviceStatistics",
        "iotwireless:getWirelessGateway",
        "iotwireless:getWirelessGatewayCertificate",
        "iotwireless:getWirelessGatewayFirmwareInformation",
        "iotwireless:getWirelessGatewayStatistics",
        "iotwireless:getWirelessGatewayTask",
        "iotwireless:getWirelessGatewayTaskDefinition",
        "iotwireless:listDestinations",
        "iotwireless:listDeviceProfiles",
        "iotwireless:listPartnerAccounts",
        "iotwireless:listServiceProfiles",
        "iotwireless:listTagsForResource",
        "iotwireless:listWirelessDevices",
        "iotwireless:listWirelessGateways",
        "iotwireless:listWirelessGatewayTaskDefinitions",
```

```
        "ivs:getChannel",
        "ivs:getRecordingConfiguration",
        "ivs:getStream",
        "ivs:getStreamSession",
        "ivs:listChannels",
        "ivs:listPlaybackKeyPairs",
        "ivs:listRecordingConfigurations",
        "ivs:listStreamKeys",
        "ivs:listStreams",
        "ivs:listStreamSessions",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
        "kafka:describeTopic",
        "kafka:describeTopicPartitions",
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listTagsForResource",
        "kafka:listTopics",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "kendra:describeAccessControlConfiguration",
        "kendra:describeDataSource",
        "kendra:describeExperience",
```

```
        "kendra:describeFaq",
        "kendra:describeFeaturedResultsSet",
        "kendra:describeIndex",
        "kendra:describePrincipalMapping",
        "kendra:describeQuerySuggestionsBlockList",
        "kendra:describeQuerySuggestionsConfig",
        "kendra:describeThesaurus",
        "kendra:listAccessControlConfigurations",
        "kendra:listDataSourceSyncJobs",
        "kendra:listDataSources",
        "kendra:listEntityPersonas",
        "kendra:listExperienceEntities",
        "kendra:listExperiences",
        "kendra:listFaqs",
        "kendra:listFeaturedResultsSets",
        "kendra:listIndices",
        "kendra:listQuerySuggestionsBlockLists",
        "kendra:listThesauri",
        "kinesis:describeStream",
        "kinesis:describeStreamConsumer",
        "kinesis:describeStreamSummary",
        "kinesis:listShards",
        "kinesis:listStreamConsumers",
        "kinesis:listStreams",
        "kinesis:listTagsForStream",
        "kinesisanalytics:describeApplication",
        "kinesisanalytics:describeApplicationOperation",
        "kinesisanalytics:describeApplicationSnapshot",
        "kinesisanalytics:listApplicationOperations",
        "kinesisanalytics:listApplications",
        "kinesisanalytics:listApplicationSnapshots",
        "kinesisanalytics:listApplicationVersions",
        "kinesisvideo:describeImageGenerationConfiguration",
        "kinesisvideo:describeEdgeConfiguration",
        "kinesisvideo:describeMappedResourceConfiguration",
        "kinesisvideo:describeMediaStorageConfiguration",
        "kinesisvideo:describeNotificationConfiguration",
        "kinesisvideo:describeSignalingChannel",
        "kinesisvideo:describeStream",
        "kinesisvideo:getDataEndpoint",
        "kinesisvideo:getIceServerConfig",
        "kinesisvideo:getSignalingChannelEndpoint",
        "kinesisvideo:listSignalingChannels",
        "kinesisvideo:listEdgeAgentConfigurations",
```

```
        "kinesisvideo:listStreams",
        "kms:describeCustomKeyStores",
        "kms:describeKey",
        "kms:getKeyPolicy",
        "kms:getKeyRotationStatus",
        "kms:listAliases",
        "kms:listGrants",
        "kms:listKeyPolicies",
        "kms:listKeyRotations",
        "kms:listKeys",
        "kms:listResourceTags",
        "kms:listRetirableGrants",
        "lakeformation:describeLakeFormationIdentityCenterConfiguration",
        "lakeformation:describeResource",
        "lakeformation:describeTransaction",
        "lakeformation:getDataLakePrincipal",
        "lakeformation:getDataLakeSettings",
        "lakeformation:getEffectivePermissionsForPath",
        "lakeformation:getLFTag",
        "lakeformation:getLFTagExpression",
        "lakeformation:getQueryState",
        "lakeformation:getQueryStatistics",
        "lakeformation:getResourceLFTags",
        "lakeformation:listLFTagExpressions",
        "lakeformation:listLFTags",
        "lakeformation:listLakeFormationOptIns",
        "lakeformation:listPermissions",
        "lakeformation:listResources",
        "lakeformation:searchDatabasesByLFTags",
        "lakeformation:searchTablesByLFTags",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getDurableExecution",
        "lambda:getDurableExecutionHistory",
        "lambda:getDurableExecutionState",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionRecursionConfig",
        "lambda:getFunctionScalingConfig",
```

```
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getCapacityProvider",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCapacityProviders",
        "lambda:listCodeSigningConfigs",
        "lambda:listDurableExecutionsByFunction",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listFunctionUrlConfigs",
        "lambda:listFunctionVersionsByCapacityProvider",
        "lambda:listLayers",
        "lambda:listLayerVersions",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listTags",
        "lambda:listVersionsByFunction",
        "launchwizard:describeProvisionedApp",
        "launchwizard:describeProvisioningEvents",
        "launchwizard:listDeploymentEvents",
        "launchwizard:listDeployments",
        "launchwizard:listProvisionedApps",
        "lex:describeBot",
        "lex:describeBotAlias",
        "lex:describeBotLocale",
        "lex:describeBotRecommendation",
        "lex:describeBotVersion",
        "lex:describeCustomVocabularyMetadata",
        "lex:describeExport",
        "lex:describeImport",
        "lex:describeIntent",
        "lex:describeResourcePolicy",
        "lex:describeSlot",
        "lex:describeSlotType",
        "lex:getBot",
        "lex:getBotAlias",
        "lex:getBotAliases",
        "lex:getBotChannelAssociation",
        "lex:getBotChannelAssociations",
```

```
        "lex:getBots",
        "lex:getBotVersions",
        "lex:getBuiltinIntent",
        "lex:getBuiltinIntents",
        "lex:getBuiltinSlotTypes",
        "lex:getIntent",
        "lex:getIntents",
        "lex:getIntentVersions",
        "lex:getSlotType",
        "lex:getSlotTypes",
        "lex:getSlotTypeVersions",
        "lex:listBotAliases",
        "lex:listBotLocales",
        "lex:listBotRecommendations",
        "lex:listBots",
        "lex:listBotVersions",
        "lex:listExports",
        "lex:listImports",
        "lex:listIntents",
        "lex:listRecommendedIntents",
        "lex:listSlots",
        "lex:listSlotTypes",
        "license-manager:getGrant",
        "license-manager:getLicense",
        "license-manager:getLicenseConfiguration",
        "license-manager:getLicenseConversionTask",
        "license-manager:getLicenseManagerReportGenerator",
        "license-manager:getLicenseUsage",
        "license-manager:getServiceSettings",
        "license-manager:listAssociationsForLicenseConfiguration",
        "license-manager:listDistributedGrants",
        "license-manager:listFailuresForLicenseConfigurationOperations",
        "license-manager:listLicenseConfigurations",
        "license-manager:listLicenseConversionTasks",
        "license-manager:listLicenseManagerReportGenerators",
        "license-manager:listLicenses",
        "license-manager:listLicenseSpecificationsForResource",
        "license-manager:listLicenseVersions",
        "license-manager:listReceivedGrants",
        "license-manager:listReceivedGrantsForOrganization",
        "license-manager:listReceivedLicenses",
        "license-manager:listReceivedLicensesForOrganization",
        "license-manager:listResourceInventory",
        "license-manager:listTokens",
```

```
        "license-manager:listUsageForLicenseConfiguration",
        "license-manager-linux-subscriptions:getRegisteredSubscriptionProvider",
        "license-manager-linux-subscriptions:getServiceSettings",
        "license-manager-linux-subscriptions:listLinuxSubscriptionInstances",
        "license-manager-linux-subscriptions:listLinuxSubscriptions",
        "license-manager-linux-subscriptions:listRegisteredSubscriptionProviders",
        "license-manager-user-subscriptions:listIdentityProviders",
        "license-manager-user-subscriptions:listInstances",
        "license-manager-user-subscriptions:listLicenseServerEndpoints",
        "license-manager-user-subscriptions:listProductSubscriptions",
        "license-manager-user-subscriptions:listUserAssociations",
        "lightsail:getActiveNames",
        "lightsail:getAlarms",
        "lightsail:getAutoSnapshots",
        "lightsail:getBlueprints",
        "lightsail:getBucketBundles",
        "lightsail:getBucketMetricData",
        "lightsail:getBuckets",
        "lightsail:getBundles",
        "lightsail:getCertificates",
        "lightsail:getContainerImages",
        "lightsail:getContainerServiceDeployments",
        "lightsail:getContainerServiceMetricData",
        "lightsail:getContainerServicePowers",
        "lightsail:getContainerServices",
        "lightsail:getDisk",
        "lightsail:getDisks",
        "lightsail:getDiskSnapshot",
        "lightsail:getDiskSnapshots",
        "lightsail:getDistributionBundles",
        "lightsail:getDistributionMetricData",
        "lightsail:getDistributions",
        "lightsail:getDomain",
        "lightsail:getDomains",
        "lightsail:getExportSnapshotRecords",
        "lightsail:getInstance",
        "lightsail:getInstanceMetricData",
        "lightsail:getInstancePortStates",
        "lightsail:getInstances",
        "lightsail:getInstanceSnapshot",
        "lightsail:getInstanceSnapshots",
        "lightsail:getInstanceState",
        "lightsail:getKeyPair",
        "lightsail:getKeyPairs",
```

```
        "lightsail:getLoadBalancer",
        "lightsail:getLoadBalancerMetricData",
        "lightsail:getLoadBalancers",
        "lightsail:getLoadBalancerTlsCertificates",
        "lightsail:getOperation",
        "lightsail:getOperations",
        "lightsail:getOperationsForResource",
        "lightsail:getRegions",
        "lightsail:getRelationalDatabase",
        "lightsail:getRelationalDatabaseMetricData",
        "lightsail:getRelationalDatabases",
        "lightsail:getRelationalDatabaseSnapshot",
        "lightsail:getRelationalDatabaseSnapshots",
        "lightsail:getStaticIp",
        "lightsail:getStaticIps",
        "lightsail:isVpcPeered",
        "logs:describeAccountPolicies",
        "logs:describeDeliveries",
        "logs:describeDeliveryDestinations",
        "logs:describeDeliverySources",
        "logs:describeDestinations",
        "logs:describeExportTasks",
        "logs:describeFieldIndexes",
        "logs:describeIndexPolicies",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeQueries",
        "logs:describeQueryDefinitions",
        "logs:describeResourcePolicies",
        "logs:describeSubscriptionFilters",
        "logs:getDataProtectionPolicy",
        "logs:getDelivery",
        "logs:getDeliveryDestination",
        "logs:getDeliveryDestinationPolicy",
        "logs:getDeliverySource",
        "logs:getIntegration",
        "logs:getLogAnomalyDetector",
        "logs:getLogDelivery",
        "logs:getLogGroupFields",
        "logs:getTransformer",
        "logs:listAnomalies",
        "logs:listIntegrations",
        "logs:listLogAnomalyDetectors",
```

```
        "logs:listLogDeliveries",
        "logs:listLogGroupsForQuery",
        "logs:testMetricFilter",
        "lookoutequipment:describeDataIngestionJob",
        "lookoutequipment:describeDataset",
        "lookoutequipment:describeInferenceScheduler",
        "lookoutequipment:describeModel",
        "lookoutequipment:listDataIngestionJobs",
        "lookoutequipment:listDatasets",
        "lookoutequipment:listInferenceExecutions",
        "lookoutequipment:listInferenceSchedulers",
        "lookoutequipment:listModels",
        "m2:getApplication",
        "m2:getApplicationVersion",
        "m2:getBatchJobExecution",
        "m2:getDataSetDetails",
        "m2:getDataSetImportTask",
        "m2:getDeployment",
        "m2:getEnvironment",
        "m2:listApplications",
        "m2:listApplicationVersions",
        "m2:listBatchJobDefinitions",
        "m2:listBatchJobExecutions",
        "m2:listDataSetImportHistory",
        "m2:listDataSets",
        "m2:listDeployments",
        "m2:listEngineVersions",
        "m2:listEnvironments",
        "machinelearning:describeBatchPredictions",
        "machinelearning:describeDataSources",
        "machinelearning:describeEvaluations",
        "machinelearning:describeMLModels",
        "machinelearning:getBatchPrediction",
        "machinelearning:getDataSource",
        "machinelearning:getEvaluation",
        "machinelearning:getMLModel",
        "macie2:describeBuckets",
        "macie2:describeClassificationJob",
        "macie2:getAdministratorAccount",
        "macie2:getAllowList",
        "macie2:getAutomatedDiscoveryConfiguration",
        "macie2:getClassificationExportConfiguration",
        "macie2:getClassificationScope",
        "macie2:getCustomDataIdentifier",
```

```
        "macie2:getFindings",
        "macie2:getFindingsFilter",
        "macie2:getFindingsPublicationConfiguration",
        "macie2:getFindingStatistics",
        "macie2:getMacieSession",
        "macie2:getMember",
        "macie2:getResourceProfile",
        "macie2:getRevealConfiguration",
        "macie2:getSensitivityInspectionTemplate",
        "macie2:getUsageStatistics",
        "macie2:listAllowLists",
        "macie2:listAutomatedDiscoveryAccounts",
        "macie2:listClassificationJobs",
        "macie2:listClassificationScopes",
        "macie2:listCustomDataIdentifiers",
        "macie2:listFindings",
        "macie2:listFindingsFilters",
        "macie2:listMembers",
        "macie2:listSensitivityInspectionTemplates",
        "managedblockchain:getMember",
        "managedblockchain:getNetwork",
        "managedblockchain:getNode",
        "managedblockchain:listMembers",
        "managedblockchain:listNetworks",
        "managedblockchain:listNodes",
        "mediaconnect:describeFlow",
        "mediaconnect:listEntitlements",
        "mediaconnect:listFlows",
        "mediaconvert:describeEndpoints",
        "mediaconvert:getJob",
        "mediaconvert:getJobTemplate",
        "mediaconvert:getPreset",
        "mediaconvert:getQueue",
        "mediaconvert:listJobs",
        "mediaconvert:listJobTemplates",
        "medialive:describeChannel",
        "medialive:describeInput",
        "medialive:describeInputDevice",
        "medialive:describeInputSecurityGroup",
        "medialive:describeMultiplex",
        "medialive:describeOffering",
        "medialive:describeReservation",
        "medialive:describeSchedule",
        "medialive:getCloudWatchAlarmTemplate",
```

```
        "medialive:getCloudWatchAlarmTemplateGroup",
        "medialive:getEventBridgeRuleTemplate",
        "medialive:getEventBridgeRuleTemplateGroup",
        "medialive:getSignalMap",
        "medialive:listChannels",
        "medialive:listCloudWatchAlarmTemplateGroups",
        "medialive:listCloudWatchAlarmTemplates",
        "medialive:listEventBridgeRuleTemplateGroups",
        "medialive:listEventBridgeRuleTemplates",
        "medialive:listInputDevices",
        "medialive:listInputs",
        "medialive:listInputSecurityGroups",
        "medialive:listMultiplexes",
        "medialive:listOfferings",
        "medialive:listReservations",
        "medialive:listSignalMaps",
        "mediapackage:describeChannel",
        "mediapackage:describeOriginEndpoint",
        "mediapackage:listChannels",
        "mediapackage:listOriginEndpoints",
        "mediastore:describeContainer",
        "mediastore:getContainerPolicy",
        "mediastore:getCorsPolicy",
        "mediastore:listContainers",
        "mediatailor:getPlaybackConfiguration",
        "mediatailor:listPlaybackConfigurations",
        "medical-imaging:getDatastore",
        "medical-imaging:listDatastores",
        "memorydb:describeReservedNodesOfferings",
        "memorydb:listAllowedNodeTypeUpdates",
        "mgn:describeJobLogItems",
        "mgn:describeJobs",
        "mgn:describeLaunchConfigurationTemplates",
        "mgn:describeReplicationConfigurationTemplates",
        "mgn:describeSourceServers",
        "mgn:describeVcenterClients",
        "mgn:getLaunchConfiguration",
        "mgn:getReplicationConfiguration",
        "mgn:listApplications",
        "mgn:listSourceServerActions",
        "mgn:listTemplateActions",
        "mgn:listWaves",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
```

```
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApp",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getCampaignVersion",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEndpoint",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJob",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJob",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSegmentVersion",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "mobiletargeting:phoneNumberValidate",
        "mpa:getApprovalTeam",
        "mpa:getSession",
        "mpa:listApprovalTeams",
        "mq:describeBrokerInstanceOptions",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
```

```
        "mq:listConfigurations",
        "mq:listUsers",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeFlowOperation",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeResourcePolicy",
        "network-firewall:describeRuleGroup",
        "network-firewall:describeRuleGroupMetadata",
        "network-firewall:describeTlsInspectionConfiguration",
        "network-firewall:describeVpcEndpointAssociation",
        "network-firewall:listAnalysisReports",
        "network-firewall:listFirewallPolicies",
        "network-firewall:listFirewalls",
        "network-firewall:listFlowOperationResults",
        "network-firewall:listFlowOperations",
        "network-firewall:listRuleGroups",
        "network-firewall:listTlsInspectionConfigurations",
        "network-firewall:listVpcEndpointAssociations",
        "networkflowmonitor:getMonitor",
        "networkflowmonitor:getScope",
        "networkflowmonitor:listMonitors",
        "networkflowmonitor:listScopes",
        "networkmanager:describeGlobalNetworks",
        "networkmanager:getConnectAttachment",
        "networkmanager:getConnections",
        "networkmanager:getConnectPeer",
        "networkmanager:getConnectPeerAssociations",
        "networkmanager:getCoreNetwork",
        "networkmanager:getCoreNetworkChangeEvents",
        "networkmanager:getCoreNetworkChangeSet",
        "networkmanager:getCoreNetworkPolicy",
        "networkmanager:getCustomerGatewayAssociations",
        "networkmanager:getDevices",
        "networkmanager:getDirectConnectGatewayAttachment",
        "networkmanager:getLinkAssociations",
        "networkmanager:getLinks",
        "networkmanager:getNetworkResourceCounts",
        "networkmanager:getNetworkResourceRelationships",
        "networkmanager:getNetworkResources",
        "networkmanager:getNetworkRoutes",
        "networkmanager:getNetworkTelemetry",
        "networkmanager:getResourcePolicy",
        "networkmanager:getRouteAnalysis",
```

```
        "networkmanager:getSites",
        "networkmanager:getSiteToSiteVpnAttachment",
        "networkmanager:getTransitGatewayConnectPeerAssociations",
        "networkmanager:getTransitGatewayPeering",
        "networkmanager:getTransitGatewayRegistrations",
        "networkmanager:getTransitGatewayRouteTableAttachment",
        "networkmanager:getVpcAttachment",
        "networkmanager:listAttachments",
        "networkmanager:listConnectPeers",
        "networkmanager:listCoreNetworkPolicyVersions",
        "networkmanager:listCoreNetworks",
        "networkmanager:listOrganizationServiceAccessStatus",
        "networkmanager:listPeerings",
        "networkmanager:listTagsForResource",
        "networkmonitor:getMonitor",
        "networkmonitor:getProbe",
        "networkmonitor:listMonitors",
        "notifications-contacts:getEmailContact",
        "notifications-contacts:listEmailContacts",
        "notifications:getEventRule",
        "notifications:getNotificationConfiguration",
        "notifications:getNotificationEvent",
        "notifications:listChannels",
        "notifications:listEventRules",
        "notifications:listNotificationConfigurations",
        "notifications:listNotificationEvents",
        "notifications:listNotificationHubs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup3",
      "Effect" : "Allow",
      "Action" : [
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "observabilityadmin:getTelemetryEvaluationStatus",
        "observabilityadmin:getTelemetryEvaluationStatusForOrganization",
```

```
        "observabilityadmin:listResourceTelemetry",
        "observabilityadmin:listResourceTelemetryForOrganization",
        "odb:getCloudAutonomousVmCluster",
        "odb:getCloudVmCluster",
        "odb:getOciOnboardingStatus",
        "odb:getOdbNetwork",
        "odb:getOdbPeeringConnection",
        "odb:listCloudAutonomousVmClusters",
        "odb:listCloudVmClusters",
        "odb:listOdbNetworks",
        "odb:listOdbPeeringConnections",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getAnnotationStoreVersion",
        "omics:getReadSetActivationJob",
        "omics:getReadSetExportJob",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunCache",
        "omics:getRunGroup",
        "omics:getRunTask",
        "omics:getSequenceStore",
        "omics:getShare",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:getWorkflowVersion",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listAnnotationStoreVersions",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetActivationJobs",
        "omics:listReadSetExportJobs",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferences",
        "omics:listReferenceStores",
```

```
        "omics:listRunCaches",
        "omics:listRunGroups",
        "omics:listRuns",
        "omics:listRunTasks",
        "omics:listSequenceStores",
        "omics:listShares",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
        "omics:listWorkflows",
        "omics:listWorkflowVersions",
        "opsworks-cm:describeAccountAttributes",
        "opsworks-cm:describeBackups",
        "opsworks-cm:describeEvents",
        "opsworks-cm:describeNodeAssociationStatus",
        "opsworks-cm:describeServers",
        "opsworks:describeAgentVersions",
        "opsworks:describeApps",
        "opsworks:describeCommands",
        "opsworks:describeDeployments",
        "opsworks:describeEcsClusters",
        "opsworks:describeElasticIps",
        "opsworks:describeElasticLoadBalancers",
        "opsworks:describeInstances",
        "opsworks:describeLayers",
        "opsworks:describeLoadBasedAutoScaling",
        "opsworks:describeMyUserProfile",
        "opsworks:describePermissions",
        "opsworks:describeRaidArrays",
        "opsworks:describeRdsDbInstances",
        "opsworks:describeServiceErrors",
        "opsworks:describeStackProvisioningParameters",
        "opsworks:describeStacks",
        "opsworks:describeStackSummary",
        "opsworks:describeTimeBasedAutoScaling",
        "opsworks:describeUserProfiles",
        "opsworks:describeVolumes",
        "opsworks:getHostnameSuggestion",
        "organizations:describeAccount",
        "organizations:describeCreateAccountStatus",
        "organizations:describeEffectivePolicy",
        "organizations:describeHandshake",
        "organizations:describeOrganization",
        "organizations:describeOrganizationalUnit",
        "organizations:describePolicy",
```

```
        "organizations:describeResourcePolicy",
        "organizations:listAccounts",
        "organizations:listAccountsForParent",
        "organizations:listAWSServiceAccessForOrganization",
        "organizations:listChildren",
        "organizations:listCreateAccountStatus",
        "organizations:listDelegatedAdministrators",
        "organizations:listDelegatedServicesForAccount",
        "organizations:listHandshakesForAccount",
        "organizations:listHandshakesForOrganization",
        "organizations:listOrganizationalUnitsForParent",
        "organizations:listParents",
        "organizations:listPolicies",
        "organizations:listPoliciesForTarget",
        "organizations:listRoots",
        "organizations:listTagsForResource",
        "organizations:listTargetsForPolicy",
        "osis:getPipeline",
        "osis:getPipelineBlueprint",
        "osis:getPipelineChangeProgress",
        "osis:listPipelineBlueprints",
        "osis:listPipelines",
        "osis:validatePipeline",
        "outposts:getCapacityTask",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getOutpostSupportedInstanceTypes",
        "outposts:getSite",
        "outposts:listAssets",
        "outposts:listAssetInstances",
        "outposts:listBlockingInstancesForCapacityTask",
        "outposts:listCapacityTasks",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "payment-cryptography:getAlias",
        "payment-cryptography:getKey",
        "payment-cryptography:listAliases",
        "payment-cryptography:listKeys",
        "pca-connector-ad:listConnectors",
```

```
        "pca-connector-ad:listDirectoryRegistrations",
        "pca-connector-ad:listServicePrincipalNames",
        "pca-connector-ad:listTagsForResource",
        "pca-connector-ad:listTemplateGroupAccessControlEntries",
        "pca-connector-ad:listTemplates",
        "pcs:getCluster",
        "pcs:getComputeNodeGroup",
        "pcs:getQueue",
        "pcs:listClusters",
        "pcs:listComputeNodeGroups",
        "pcs:listQueues",
        "personalize:describeAlgorithm",
        "personalize:describeBatchInferenceJob",
        "personalize:describeBatchSegmentJob",
        "personalize:describeCampaign",
        "personalize:describeDataInsightsJob",
        "personalize:describeDataset",
        "personalize:describeDatasetExportJob",
        "personalize:describeDatasetGroup",
        "personalize:describeDatasetImportJob",
        "personalize:describeEventTracker",
        "personalize:describeFeatureTransformation",
        "personalize:describeFilter",
        "personalize:describeMetricAttribution",
        "personalize:describeRecipe",
        "personalize:describeRecommender",
        "personalize:describeSchema",
        "personalize:describeSolution",
        "personalize:describeSolutionVersion",
        "personalize:getPersonalizedRanking",
        "personalize:getRecommendations",
        "personalize:getSolutionMetrics",
        "personalize:listBatchInferenceJobs",
        "personalize:listBatchSegmentJobs",
        "personalize:listCampaigns",
        "personalize:listDataInsightsJobs",
        "personalize:listDatasetExportJobs",
        "personalize:listDatasetGroups",
        "personalize:listDatasetImportJobs",
        "personalize:listDatasets",
        "personalize:listEventTrackers",
        "personalize:listMetricAttributions",
        "personalize:listRecipes",
        "personalize:listRecommenders",
```

```
        "personalize:listSchemas",
        "personalize:listSolutions",
        "personalize:listSolutionVersions",
        "pipes:describePipe",
        "pipes:listPipes",
        "pipes:listTagsForResource",
        "polly:describeVoices",
        "polly:getLexicon",
        "polly:listLexicons",
        "pricing:describeServices",
        "pricing:getAttributeValues",
        "pricing:getProducts",
        "private-networks:getDeviceIdentifier",
        "private-networks:getNetwork",
        "private-networks:getNetworkResource",
        "private-networks:listDeviceIdentifiers",
        "private-networks:listNetworkResources",
        "private-networks:listNetworks",
        "qbusiness:getApplication",
        "qbusiness:getDataSource",
        "qbusiness:getIndex",
        "qbusiness:getRetriever",
        "qbusiness:getWebExperience",
        "qbusiness:listApplications",
        "qbusiness:listDataSources",
        "qbusiness:listDataSourceSyncJobs",
        "qbusiness:listIndices",
        "qbusiness:listRetrievers",
        "qbusiness:listWebExperiences",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetPermissions",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeDataSourcePermissions",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
```

```
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicPermissions",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboards",
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
        "quicksight:listThemeVersions",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
```

```
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterAutomatedBackups",
        "rds:describeDBClusterBacktracks",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusterSnapshotAttributes",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBMajorEngineVersions",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBProxies",
        "rds:describeDBProxyEndpoints",
        "rds:describeDBProxyTargetGroups",
        "rds:describeDBProxyTargets",
        "rds:describeDBRecommendations",
        "rds:describeDBSecurityGroups",
        "rds:describeDBShardGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSnapshotTenantDatabases",
```

```
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEvents",
        "rds:describeEventSubscriptions",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeTenantDatabases",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift-serverless:getCustomDomainAssociation",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getScheduledAction",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listCustomDomainAssociations",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshotCopyConfigurations",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "redshift:describeClusterDbRevisions",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
```

```
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterTracks",
        "redshift:describeClusterVersions",
        "redshift:describeCustomDomainAssociations",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEndpointAccess",
        "redshift:describeEndpointAuthorization",
        "redshift:describeEventCategories",
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeInboundIntegrations",
        "redshift:describeLoggingStatus",
        "redshift:describeNodeConfigurationOptions",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeRedshiftIdcApplications",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeSnapshotSchedules",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift:describeUsageLimits",
        "rekognition:listCollections",
        "rekognition:listFaces",
        "resiliencehub:describeApp",
        "resiliencehub:describeAppAssessment",
        "resiliencehub:describeAppVersion",
        "resiliencehub:describeAppVersionAppComponent",
        "resiliencehub:describeAppVersionResource",
        "resiliencehub:describeAppVersionResourcesResolutionStatus",
        "resiliencehub:describeAppVersionTemplate",
        "resiliencehub:describeDraftAppVersionResourcesImportStatus",
        "resiliencehub:describeResiliencyPolicy",
        "resiliencehub:describeResourceGroupingRecommendationTask",
        "resiliencehub:listAlarmRecommendations",
        "resiliencehub:listAppAssessmentComplianceDrifts",
```

```
        "resiliencehub:listAppAssessmentResourceDrifts",
        "resiliencehub:listAppAssessments",
        "resiliencehub:listAppComponentCompliances",
        "resiliencehub:listAppComponentRecommendations",
        "resiliencehub:listAppInputSources",
        "resiliencehub:listApps",
        "resiliencehub:listAppVersionAppComponents",
        "resiliencehub:listAppVersionResourceMappings",
        "resiliencehub:listAppVersionResources",
        "resiliencehub:listAppVersions",
        "resiliencehub:listRecommendationTemplates",
        "resiliencehub:listResiliencyPolicies",
        "resiliencehub:listResourceGroupingRecommendations",
        "resiliencehub:listSopRecommendations",
        "resiliencehub:listSuggestedResiliencyPolicies",
        "resiliencehub:listTestRecommendations",
        "resiliencehub:listUnsupportedAppVersionResources",
        "resource-explorer-2:getAccountLevelServiceConfiguration",
        "resource-explorer-2:getIndex",
        "resource-explorer-2:getView",
        "resource-explorer-2:listIndexes",
        "resource-explorer-2:listViews",
        "resource-explorer-2:search",
        "resource-groups:getGroup",
        "resource-groups:getGroupQuery",
        "resource-groups:getTags",
        "resource-groups:listGroupResources",
        "resource-groups:listGroups",
        "resource-groups:searchResources",
        "robomaker:batchDescribeSimulationJob",
        "robomaker:describeDeploymentJob",
        "robomaker:describeFleet",
        "robomaker:describeRobot",
        "robomaker:describeRobotApplication",
        "robomaker:describeSimulationApplication",
        "robomaker:describeSimulationJob",
        "robomaker:listDeploymentJobs",
        "robomaker:listFleets",
        "robomaker:listRobotApplications",
        "robomaker:listRobots",
        "robomaker:listSimulationApplications",
        "robomaker:listSimulationJobs",
        "rolesanywhere:getProfile",
        "rolesanywhere:getTrustAnchor",
```

```
        "rolesanywhere:listProfiles",
        "rolesanywhere:listTrustAnchors",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeCluster",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:getResourcePolicy",
        "route53-recovery-control-config:listAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:listClusters",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getArchitectureRecommendations",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listCrossAccountAuthorizations",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53-recovery-readiness:listRules",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
```

```
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53profiles:getProfile",
        "route53profiles:getProfileAssociation",
        "route53profiles:getProfileResourceAssociation",
        "route53profiles:listProfileAssociations",
        "route53profiles:listProfileResourceAssociations",
        "route53profiles:listProfiles",
        "route53profiles:listTagsForResource",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverConfig",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverEndpoint",
        "route53resolver:getResolverQueryLogConfig",
```

```
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "route53globalresolver:getAccessSource",
        "route53globalresolver:getAccessToken",
        "route53globalresolver:getDNSView",
        "route53globalresolver:getFirewallDomainList",
        "route53globalresolver:getFirewallRule",
        "route53globalresolver:getGlobalResolver",
        "route53globalresolver:getHostedZoneAssociation",
        "route53globalresolver:getManagedFirewallDomainList",
        "route53globalresolver:listAccessSources",
        "route53globalresolver:listAccessTokens",
        "route53globalresolver:listDNSViews",
        "route53globalresolver:listFirewallDomainLists",
        "route53globalresolver:listFirewallDomains",
        "route53globalresolver:listFirewallRules",
        "route53globalresolver:listGlobalResolvers",
        "route53globalresolver:listHostedZoneAssociations",
        "route53globalresolver:listManagedFirewallDomainLists",
        "rum:batchGetRumMetricDefinitions",
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
        "s3-outposts:getLifecycleConfiguration",
        "s3-outposts:getAccessPoint",
```

```
        "s3-outposts:getAccessPointPolicy",
        "s3-outposts:getBucketPolicy",
        "s3-outposts:getBucketVersioning",
        "s3-outposts:getReplicationConfiguration",
        "s3-outposts:listAccessPoints",
        "s3-outposts:listEndpoints",
        "s3-outposts:listOutpostsWithS3",
        "s3-outposts:listRegionalBuckets",
        "s3-outposts:listSharedEndpoints",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessGrant",
        "s3:getAccessGrantsInstance",
        "s3:getAccessGrantsInstanceResourcePolicy",
        "s3:getAccessGrantsLocation",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
```

```
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectAcl",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessGrants",
        "s3:listAccessGrantsInstances",
        "s3:listAccessGrantsLocations",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultipartUploadParts",
        "s3:listMultiRegionAccessPoints",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
        "s3express:listAllMyDirectoryBuckets",
        "s3tables:getNamespace",
        "s3tables:getTable",
        "s3tables:getTableBucket",
        "s3tables:getTableBucketEncryption",
        "s3tables:getTableBucketMaintenanceConfiguration",
        "s3tables:getTableBucketMetricsConfiguration",
        "s3tables:getTableBucketPolicy",
        "s3tables:getTableBucketReplication",
        "s3tables:getTableBucketStorageClass",
        "s3tables:getTableEncryption",
        "s3tables:getTableMaintenanceConfiguration",
        "s3tables:getTableMaintenanceJobStatus",
        "s3tables:getTableMetadataLocation",
        "s3tables:getTablePolicy",
        "s3tables:getTableRecordExpirationConfiguration",
        "s3tables:getTableRecordExpirationJobStatus",
        "s3tables:getTableReplication",
        "s3tables:getTableReplicationStatus",
        "s3tables:getTableStorageClass",
        "s3tables:listNamespaces",
        "s3tables:listTableBuckets",
```

```
        "s3tables:listTables",
        "s3vectors:getIndex",
        "s3vectors:getVectorBucket",
        "s3vectors:getVectorBucketPolicy",
        "s3vectors:listIndexes",
        "s3vectors:listVectorBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeAutoMLJobV2",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeClusterEvent",
        "sagemaker:describeClusterSchedulerConfig",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeComputeQuota",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeLineageGroup",
```

```
        "sagemaker:describeMlflowApp",
        "sagemaker:describeMlflowTrackingServer",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describeOptimizationJob",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describePartnerApp",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeReservedCapacity",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTrainingPlan",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getLineageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
```

```
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listClusterEvents",
        "sagemaker:listClusterSchedulerConfigs",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listComputeQuotas",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContents",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImages",
        "sagemaker:listImageVersions",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listMlflowApps",
        "sagemaker:listMlflowTrackingServers",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCards",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
```

```
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listOptimizationJobs",
        "sagemaker:listPartnerApps",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listPipelineVersions",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listResourceCatalogs",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTrainingPlans",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listUltraServersByReservedCapacity",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "sagemaker:search",
        "savingsplans:describeSavingsPlans",
        "scheduler:getSchedule",
        "scheduler:getScheduleGroup",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "schemas:describeCodeBinding",
        "schemas:describeDiscoverer",
        "schemas:describeRegistry",
        "schemas:describeSchema",
        "schemas:getCodeBindingSource",
```

```
        "schemas:getDiscoveredSchema",
        "schemas:getResourcePolicy",
        "schemas:listDiscoverers",
        "schemas:listRegistries",
        "schemas:listSchemas",
        "schemas:listSchemaVersions",
        "sdb:domainMetadata",
        "sdb:listDomains",
        "secretsmanager:describeSecret",
        "secretsmanager:getResourcePolicy",
        "secretsmanager:listSecrets",
        "secretsmanager:listSecretVersionIds",
        "security-ir:batchGetMemberAccountDetails",
        "security-ir:getMembership",
        "security-ir:listCases",
        "security-ir:listMemberships",
        "securityhub:batchGetAutomationRules",
        "securityhub:batchGetConfigurationPolicyAssociations",
        "securityhub:describeHub",
        "securityhub:describeOrganizationConfiguration",
        "securityhub:describeProductsV2",
        "securityhub:describeSecurityHubV2",
        "securityhub:getConfigurationPolicy",
        "securityhub:getConfigurationPolicyAssociation",
        "securityhub:getEnabledStandards",
        "securityhub:getFindingAggregator",
        "securityhub:getFindingHistory",
        "securityhub:getFindings",
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "securityhub:getAggregatorV2",
        "securityhub:getAutomationRuleV2",
        "securityhub:getConnectorV2",
        "securityhub:getResourcesV2",
        "securityhub:listAutomationRules",
        "securityhub:listConfigurationPolicies",
        "securityhub:listConfigurationPolicyAssociations",
        "securityhub:listEnabledProductsForImport",
        "securityhub:listFindingAggregators",
        "securityhub:listInvitations",
        "securityhub:listMembers",
        "securityhub:listAggregatorsV2",
```

```
        "securityhub:listAutomationRulesV2",
        "securityhub:listConnectorsV2",
        "securitylake:getDataLakeExceptionSubscription",
        "securitylake:getDataLakeOrganizationConfiguration",
        "securitylake:getDataLakeSources",
        "securitylake:getSubscriber",
        "securitylake:listDataLakeExceptions",
        "securitylake:listDataLakes",
        "securitylake:listLogSources",
        "securitylake:listSubscribers",
        "serverlessrepo:getApplication",
        "serverlessrepo:getApplicationPolicy",
        "serverlessrepo:getCloudFormationTemplate",
        "serverlessrepo:listApplicationDependencies",
        "serverlessrepo:listApplications",
        "serverlessrepo:listApplicationVersions",
        "servicecatalog:describeConstraint",
        "servicecatalog:describePortfolio",
        "servicecatalog:describeProduct",
        "servicecatalog:describeProductAsAdmin",
        "servicecatalog:describeProductView",
        "servicecatalog:describeProvisioningArtifact",
        "servicecatalog:describeProvisioningParameters",
        "servicecatalog:describeRecord",
        "servicecatalog:listAcceptedPortfolioShares",
        "servicecatalog:listConstraintsForPortfolio",
        "servicecatalog:listLaunchPaths",
        "servicecatalog:listPortfolioAccess",
        "servicecatalog:listPortfolios",
        "servicecatalog:listPortfoliosForProduct",
        "servicecatalog:listPrincipalsForPortfolio",
        "servicecatalog:listProvisioningArtifacts",
        "servicecatalog:listRecordHistory",
        "servicecatalog:scanProvisionedProducts",
        "servicecatalog:searchProducts",
        "servicequotas:getAssociationForServiceQuotaTemplate",
        "servicequotas:getAWSDefaultServiceQuota",
        "servicequotas:getRequestedServiceQuotaChange",
        "servicequotas:getServiceQuota",
        "servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listRequestedServiceQuotaChangeHistory",
        "servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
```

```
        "servicequotas:listServiceQuotas",
        "servicequotas:listServices",
        "ses:batchGetMetricData",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getAddonInstance",
        "ses:getAddonSubscription",
        "ses:getArchive",
        "ses:getArchiveExport",
        "ses:getArchiveSearch",
        "ses:getArchiveSearchResults",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getIngressPoint",
        "ses:getMessageInsights",
        "ses:getRelay",
        "ses:getRuleSet",
        "ses:getTrafficPolicy",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listAddonInstances",
        "ses:listAddonSubscriptions",
        "ses:listArchiveExports",
```

```
        "ses:listArchives",
        "ses:listArchiveSearches",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listIngressPoints",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRelays",
        "ses:listRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listTrafficPolicies",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
        "shield:describeProtection",
        "shield:describeSubscription",
        "shield:listAttacks",
        "shield:listProtections",
        "signer:describeSigningJob",
        "signer:getRevocationStatus",
        "signer:getSigningPlatform",
        "signer:getSigningProfile",
        "signer:listProfilePermissions",
        "signer:listSigningJobs",
        "signer:listSigningPlatforms",
        "signer:listSigningProfiles",
        "sms-voice:describeAccountAttributes",
        "sms-voice:describeSpendLimits",
        "sms-voice:describeVerifiedDestinationNumbers",
        "sms-voice:getConfigurationSetEventDestinations",
        "sms:getConnectors",
        "sms:getReplicationJobs",
        "sms:getReplicationRuns",
        "sms:getServers",
```

```
        "snowball:describeAddress",
        "snowball:describeAddresses",
        "snowball:describeJob",
        "snowball:getSnowballUsage",
        "snowball:listJobs",
        "snowball:listServiceVersions",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "sqs:getQueueAttributes",
        "sqs:getQueueUrl",
        "sqs:listDeadLetterSourceQueues",
        "sqs:listMessageMoveTasks",
        "sqs:listQueues",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotations",
```

```
        "ssm-contacts:listRotationShifts",
        "ssm-incidents:batchGetIncidentFindings",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentFindings",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-quicksetup:getConfiguration",
        "ssm-quicksetup:getConfigurationManager",
        "ssm-quicksetup:getServiceSettings",
        "ssm-quicksetup:listConfigurationManagers",
        "ssm-quicksetup:listConfigurations",
        "ssm-quicksetup:listQuickSetupTypes",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getConfigurationCheckOperation",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listConfigurationCheckDefinitions",
        "ssm-sap:listConfigurationCheckOperations",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "ssm-sap:listSubCheckResults",
        "ssm-sap:listSubCheckRuleResults",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutions",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
```

```
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatches",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInstanceProperties",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroups",
        "ssm:describePatchGroupState",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociations",
        "ssm:listAssociationVersions",
        "ssm:listCommandInvocations",
```

```
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocuments",
        "ssm:listDocumentVersions",
        "ssm:listNodes",
        "ssm:listNodesSummary",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "sso:describeApplication",
        "sso:describeApplicationAssignment",
        "sso:describeApplicationProvider",
        "sso:describeAccountAssignmentCreationStatus",
        "sso:describeAccountAssignmentDeletionStatus",
        "sso:describeInstance",
        "sso:describeInstanceAccessControlAttributeConfiguration",
        "sso:describePermissionSet",
        "sso:describePermissionSetProvisioningStatus",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getInlinePolicyForPermissionSet",
        "sso:getManagedApplicationInstance",
        "sso:getPermissionsBoundaryForPermissionSet",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listAccountAssignmentCreationStatus",
        "sso:listAccountAssignmentDeletionStatus",
```

```
        "sso:listAccountAssignments",
        "sso:listAccountAssignmentsForPrincipal",
        "sso:listAccountsForProvisionedPermissionSet",
        "sso:listApplicationAssignmentsForPrincipal",
        "sso:listCustomerManagedPolicyReferencesInPermissionSet",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listManagedPoliciesInPermissionSet",
        "sso:listPermissionSetProvisioningStatus",
        "sso:listPermissionSets",
        "sso:listPermissionSetsProvisionedToAccount",
        "sso:listProfileAssociations",
        "sso:listTrustedTokenIssuers",
        "states:describeActivity",
        "states:describeExecution",
        "states:describeMapRun",
        "states:describeStateMachine",
        "states:describeStateMachineAlias",
        "states:describeStateMachineForExecution",
        "states:getExecutionHistory",
        "states:listActivities",
        "states:listExecutions",
        "states:listMapRuns",
        "states:listStateMachineAliases",
        "states:listStateMachines",
        "states:listStateMachineVersions",
        "storagegateway:describeBandwidthRateLimit",
        "storagegateway:describeCache",
        "storagegateway:describeCachediSCSIVolumes",
        "storagegateway:describeFileSystemAssociations",
        "storagegateway:describeGatewayInformation",
        "storagegateway:describeMaintenanceStartTime",
        "storagegateway:describeNFSFileShares",
        "storagegateway:describeSMBFileShares",
        "storagegateway:describeSMBSettings",
        "storagegateway:describeSnapshotSchedule",
        "storagegateway:describeStorediSCSIVolumes",
        "storagegateway:describeTapeArchives",
        "storagegateway:describeTapeRecoveryPoints",
        "storagegateway:describeTapes",
        "storagegateway:describeUploadBuffer",
        "storagegateway:describeVTLDevices",
        "storagegateway:describeWorkingStorage",
        "storagegateway:listAutomaticTapeCreationPolicies",
```

```
        "storagegateway:listFileShares",
        "storagegateway:listFileSystemAssociations",
        "storagegateway:listGateways",
        "storagegateway:listLocalDisks",
        "storagegateway:listTagsForResource",
        "storagegateway:listTapes",
        "storagegateway:listVolumeInitiators",
        "storagegateway:listVolumeRecoveryPoints",
        "storagegateway:listVolumes",
        "sts:getCallerIdentity",
        "swf:countClosedWorkflowExecutions",
        "swf:countOpenWorkflowExecutions",
        "swf:countPendingActivityTasks",
        "swf:countPendingDecisionTasks",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "sustainability:getEstimatedCarbonEmissions",
        "sustainability:getEstimatedCarbonEmissionsDimensionValues",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
        "synthetics:describeRuntimeVersions",
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "tax:getTaxInheritance",
        "tax:getTaxRegistration",
        "thinclient:getDevice",
        "thinclient:getEnvironment",
        "thinclient:getSoftwareSet",
        "thinclient:listDevices",
        "thinclient:listEnvironments",
        "thinclient:listSoftwareSets",
        "timestream:describeAccountSettings",
```

```
        "timestream:describeBatchLoadTask",
        "timestream:describeDatabase",
        "timestream:describeEndpoints",
        "timestream:describeScheduledQuery",
        "timestream:describeTable",
        "timestream:listBatchLoadTasks",
        "timestream:listDatabases",
        "timestream:listScheduledQueries",
        "timestream:listTables",
        "tiros:createQuery",
        "tiros:getQueryAnswer",
        "tiros:getQueryExplanation",
        "tnb:getSolFunctionInstance",
        "tnb:getSolFunctionPackage",
        "tnb:getSolNetworkInstance",
        "tnb:getSolNetworkOperation",
        "tnb:getSolNetworkPackage",
        "tnb:listSolFunctionInstances",
        "tnb:listSolFunctionPackages",
        "tnb:listSolNetworkInstances",
        "tnb:listSolNetworkOperations",
        "tnb:listSolNetworkPackages",
        "transcribe:describeLanguageModel",
        "transcribe:getCallAnalyticsCategory",
        "transcribe:getCallAnalyticsJob",
        "transcribe:getMedicalTranscriptionJob",
        "transcribe:getMedicalVocabulary",
        "transcribe:getTranscriptionJob",
        "transcribe:getVocabulary",
        "transcribe:getVocabularyFilter",
        "transcribe:listCallAnalyticsCategories",
        "transcribe:listCallAnalyticsJobs",
        "transcribe:listLanguageModels",
        "transcribe:listMedicalTranscriptionJobs",
        "transcribe:listMedicalVocabularies",
        "transcribe:listTranscriptionJobs",
        "transcribe:listVocabularies",
        "transcribe:listVocabularyFilters",
        "transfer:describeAccess",
        "transfer:describeAgreement",
        "transfer:describeConnector",
        "transfer:describeExecution",
        "transfer:describeProfile",
        "transfer:describeServer",
```

```
        "transfer:describeUser",
        "transfer:describeWebApp",
        "transfer:describeWebAppCustomization",
        "transfer:describeWorkflow",
        "transfer:listAccesses",
        "transfer:listAgreements",
        "transfer:listConnectors",
        "transfer:listExecutions",
        "transfer:listHostKeys",
        "transfer:listProfiles",
        "transfer:listServers",
        "transfer:listTagsForResource",
        "transfer:listUsers",
        "transfer:listWebApps",
        "transfer:listWorkflows",
        "transfer:sendWorkflowStepState",
        "trustedadvisor:getOrganizationRecommendation",
        "trustedadvisor:getRecommendation",
        "trustedadvisor:listChecks",
        "trustedadvisor:listOrganizationRecommendationAccounts",
        "trustedadvisor:listOrganizationRecommendationResources",
        "trustedadvisor:listOrganizationRecommendations",
        "trustedadvisor:listRecommendationResources",
        "trustedadvisor:listRecommendations",
        "verifiedpermissions:getIdentitySource",
        "verifiedpermissions:getPolicy",
        "verifiedpermissions:getPolicyStore",
        "verifiedpermissions:getPolicyTemplate",
        "verifiedpermissions:getSchema",
        "verifiedpermissions:listIdentitySources",
        "verifiedpermissions:listPolicies",
        "verifiedpermissions:listPolicyStores",
        "verifiedpermissions:listPolicyTemplates",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getDomainVerification",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourceConfiguration",
        "vpc-lattice:getResourceGateway",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkResourceAssociation",
```

```
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listDomainVerifications",
        "vpc-lattice:listListeners",
        "vpc-lattice:listResourceConfigurations",
        "vpc-lattice:listResourceEndpointAssociations",
        "vpc-lattice:listResourceGateways",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkResourceAssociations",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServiceNetworkVpcEndpointAssociations",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
```

```
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
```

```
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workdocs:checkAlias",
        "workdocs:describeAvailableDirectories",
        "workdocs:describeInstances",
        "workmail:describeGroup",
        "workmail:describeOrganization",
        "workmail:describeResource",
        "workmail:describeUser",
        "workmail:listAliases",
        "workmail:listGroupMembers",
        "workmail:listGroups",
        "workmail:listMailboxPermissions",
        "workmail:listOrganizations",
        "workmail:listResourceDelegates",
        "workmail:listResources",
        "workmail:listUsers",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeApplicationAssociations",
        "workspaces:describeCustomWorkspaceImageImport",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
```

```
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspaceSnapshots",
        "workspaces:describeWorkspacesConnectionStatus",
        "workspaces:describeWorkspacesPools",
        "workspaces:describeWorkspacesPoolSessions",
        "xray:getEncryptionConfig",
        "xray:getGroup",
        "xray:getGroups",
        "xray:getInsightImpactGraph",
        "xray:getSamplingRules",
        "xray:getSamplingStatisticSummaries",
        "xray:getSamplingTargets",
        "xray:getServiceGraph",
        "xray:getTimeSeriesServiceStatistics",
        "xray:getTraceGraph",
        "xray:listResourcePolicies"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerAccountDiscoveryServicePolicy

Descrizione: concede a AWS Systems Manager (SSM) l'autorizzazione a scoprire Account AWS informazioni.

`AWSSystemsManagerAccountDiscoveryServicePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 24 ottobre 2019, 17:21 UTC
- Ora modificata: 17 ottobre 2022, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerChangeManagementServicePolicy

Descrizione: fornisce l'accesso alle AWS risorse gestite o utilizzate dal framework di gestione delle modifiche di AWS Systems Manager.

`AWSSystemsManagerChangeManagementServicePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 07 dicembre 2020, 22:21 UTC
- Ora modificata: 23 ottobre 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation",
        "ssm:CreateOpsItem",
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:GetCalendarState",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerEnableConfigRecordingExecutionPolicy

Descrizione: Fornisce le autorizzazioni per AWS Systems Manager Quick Setup per abilitare e configurare la registrazione della AWS configurazione Config.

`AWSSystemsManagerEnableConfigRecordingExecutionPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSystemsManagerEnableConfigRecordingExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 giugno 2024, 09:40 UTC
- Ora modificata: 26 giugno 2024, 09:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableConfigRecordingExecutionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-quick-setup-config-recording-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SNSTopicsListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultSNSTopicCreatePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ConfigRecording-Default-Topic"
    },
    {
      "Sid" : "ConfigureAndStartConfigurationRecorderPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeDeliveryChannels",
        "config:PutConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:StartConfigurationRecorder"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetAndPassConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
        "arn:aws:iam::*:role/AWSServiceRoleForConfig"
      ]
    },
    {
      "Sid" : "CreateConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerEnableExplorerExecutionPolicy

Descrizione: questo criterio concede le autorizzazioni amministrative per abilitare Explorer, una funzionalità di AWS Systems Manager. Ciò include le autorizzazioni per aggiornare le impostazioni del servizio Systems Manager correlate e per creare un ruolo collegato ai servizi per Systems Manager.

`AWSSystemsManagerEnableExplorerExecutionPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSSystemsManagerEnableExplorerExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 giugno 2024, 09:42 UTC
- Ora modificata: 26 giugno 2024, 09:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerForSAPFullAccess

Descrizione: Fornisce l'accesso completo al servizio AWS Systems Manager for SAP

`AWSSystemsManagerForSAPFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSystemsManagerForSAPFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2022, 02:11 UTC
- Ora modificata: 10 luglio 2024, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsSsmForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    },
    {
      "Sid" : "AwsSsmForSapServiceRoleCreationPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-sap.amazonaws.com/
AWSServiceRoleForAWSSSMForSAP"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm-sap.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2StartStopPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerForSAPReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura al servizio AWS Systems Manager for SAP

`AWSSystemsManagerForSAPReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSystemsManagerForSAPReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 novembre 2022, 02:11 UTC
- Ora modificata: 17 novembre 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerJustInTimeAccessServicePolicy

Descrizione: fornisce l'accesso alle AWS risorse gestite o utilizzate dal framework di accesso just in time di AWS Systems Manager.

`AWSSystemsManagerJustInTimeAccessServicePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 aprile 2025, 20:07 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerJustInTimeAccessServicePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOpsItemReplication",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOpsItemReplicationTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAutomationExecutionTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AllowOpsItemManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrieveDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : [
            "ManualApprovalPolicy",
            "AutoApprovalPolicy"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescriptions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeOpsItems",
        "ssm:DescribeSessions",
```

```
        "ssm:ListDocuments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListTagsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*"
      ]
    },
    {
      "Sid" : "AllowListSSMGUIConnections",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:ListConnections"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetUserId"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
```

```
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSOInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribingEC2Tags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPublishingCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SSM/JustInTimeAccess"
        }
      }
    },
    {
```

```
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerJustInTimeAccessTokenPolicy

Descrizione: la policy gestita AWSSystems ManagerJustInTimeAccessTokenPolicy consente a Systems Manager di generare token di accesso utilizzati per l'accesso ai just-in-time nodi.

`AWSSystemsManagerJustInTimeAccessTokenPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSystemsManagerJustInTimeAccessTokenPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 aprile 2025, 21:07 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
```

```
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "TerminateAndResumeSessionAndOpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssm:TerminateSession",
        "ssm:ResumeSession",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

Descrizione: la policy gestita AWSSystems ManagerJustInTimeAccessTokenSessionPolicy consente a Systems Manager di applicare autorizzazioni limitate a una sessione di accesso al just-in-time nodo una volta avviata.

`AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 17 aprile 2025, 20:52 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

Descrizione: questa politica consente a Systems Manager di condividere una politica di negazione dell'accesso ai just-in-time nodi dall'account amministratore delegato agli account dei membri e di replicare la politica in più regioni.

`AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 aprile 2025, 20:52 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "QuickSetupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:GetConfigurationManager",
        "cloudformation:ListStackSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ssm-quicksetup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "QuickSetupSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-quicksetup.amazonaws.com/
AWSServiceRoleForSSMQuickSetup"
      ]
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMDocumentPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:ListTagsForResource",
        "ssm:PutResourcePolicy",
        "ssm:DeleteResourcePolicy",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy"
        }
      }
    },
    {
      "Sid" : "SSMDocumentCreateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SSMDocumentUpdateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:UpdateDocumentMetadata",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
```

```
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    },
```

```
    {
      "Sid" : "RAMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : "ram:TagResource",
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RAMModificationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "SSMJustInTimeNodeAccessManagedResourceShare",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerNotificationsServicePolicy

Descrizione: autorizzazioni necessarie per raccogliere informazioni su un utente per le notifiche di Just-In-Time-Node -Access.

`AWSSystemsManagerNotificationsServicePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 aprile 2025, 20:52 UTC
- Ora modificata: 17 aprile 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerNotificationsServicePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroupMemberships",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSOActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUser",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIamActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSSystemsManagerOpsDataSyncServiceRolePolicy

Descrizione: ruolo IAM per SSM Explorer per la gestione delle operazioni OpsData correlate

`AWSSystemsManagerOpsDataSyncServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 aprile 2021, 20:42 UTC
- Ora modificata: 28 giugno 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ExplorerSecurityHubOpsItem" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:GetFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "securityhub:ASFFSyntaxPath/Workflow.Status" : "SUPPRESSED"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Confidence" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Criticality" : false
        }
      }
    },
```

```
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.Text" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.UpdatedBy" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/RelatedFindings" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Types" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.key" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.value" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/VerificationState" : false
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSThinkboxAssetServerPolicy

Descrizione: questa politica concede a AWS Portal Asset Server le autorizzazioni necessarie per il normale funzionamento.

`AWSThinkboxAssetServerPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSThinkboxAssetServerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:18 UTC
- Ora modificata: 27 maggio 2020, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
```

```
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSThinkboxAWSPortalAdminPolicy

Descrizione: questa politica garantisce al software Deadline di AWS Thinkbox l'accesso completo a più AWS servizi, come richiesto per l'amministrazione del portale. AWS Ciò include l'accesso per creare tag arbitrari su diversi tipi di risorse EC2.

`AWSThinkboxAWSPortalAdminPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSThinkboxAWSPortalAdminPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:41 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
```

```
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRegions",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetConsoleOutput",
        "ec2:ImportKeyPair",
        "ec2:ReleaseAddress",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:DisassociateAddress",
        "ec2:DeleteFleets",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteVpc",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DeleteNatGateway",
        "ec2:DetachInternetGateway",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal2",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
```

```
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal3",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/AWSPortal*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal4",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal5",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : false
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal6",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal10",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal11",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal12",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal13",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal14",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal15",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal16",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketVersioning",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3::*:awsportal*",
        "arn:aws:s3::*:stack*",
        "arn:aws:s3::*:aws-portal-cache*",
        "arn:aws:s3::*:logs-for-aws-portal-cache*",
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal17",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-aws-portal-cache*"
```

```
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal18",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal19",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal20",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal21",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stack*/*",
        "arn:aws:cloudformation:*:*:stack/Deadline*/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal22",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:EstimateTemplateCost",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal23",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal24",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal25",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal26",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : [
            "rcs-tls-pw*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal27",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSThinkboxAWSPortalGatewayPolicy

Descrizione: questo criterio concede al computer AWS Portal Gateway le autorizzazioni necessarie per il normale funzionamento.

`AWSThinkboxAWSPortalGatewayPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSThinkboxAWSPortalGatewayPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:05 UTC
- Ora modificata: 30 giugno 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "dynamodb:Scan",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSThinkboxAWSPortalWorkerPolicy

Descrizione: questa politica concede a Deadline Workers in AWS Portal le autorizzazioni necessarie per il normale funzionamento.

`AWSThinkboxAWSPortalWorkerPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSThinkboxAWSPortalWorkerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:15 UTC
- Ora modificata: 07 dicembre 2020, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineRole" : "DeadlineRenderNode"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWS*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSThinkboxDeadlineResourceTrackerAccessPolicy

Descrizione: concede le autorizzazioni necessarie per il funzionamento del Deadline Resource AWS Tracker di Thinkbox. Ciò include l'accesso completo ad alcune azioni EC2, tra cui e. DeleteFleets CancelSpotFleetRequests

`AWSThinkboxDeadlineResourceTrackerAccessPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSThinkboxDeadlineResourceTrackerAccessPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:25 UTC
- Ora modificata: 27 maggio 2020, 19:25 UTC

- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:PutItem",
        "dynamodb:Scan",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
```

```
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DeleteFleets",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeInstances",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutEvents"
      ],
      "Resource" : [
        "arn:aws:events:*:*:event-bus/default"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:ReceiveMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeStateMessageQueue*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSThinkboxDeadlineResourceTrackerAdminPolicy

Descrizione: concede le autorizzazioni necessarie per creare, distruggere e amministrare il Deadline Resource Tracker di AWS Thinkbox.

`AWSThinkboxDeadlineResourceTrackerAdminPolicy`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AWSThinkboxDeadlineResourceTrackerAdminPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:29 UTC
- Ora modificata: 16 luglio 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Versione della politica

Versione della politica: v9 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker1",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker3",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker4",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:ListTagsOfResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker5",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker6",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
      ]
```

```
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker7",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker8",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker9",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker12",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker13",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "lambda:FunctionArn" : [
            "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker14",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:Principal" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker15",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
```

```
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker16",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/deadline_aws_resource_tracker*.zip",
        "arn:aws:s3:::*/DeadlineAWSResourceTrackerTemplate*.yaml"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker17",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:TagQueue",
        "sqs:UntagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
        "arn:aws:sqs:*:*:DeadlineResourceTracker*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Descrizione: concede le autorizzazioni necessarie per il plug-in Deadline Spot Event di AWS Thinkbox. Ciò include l'autorizzazione a richiedere, modificare e annullare una flotta spot, nonché un'autorizzazione limitata. PassRole

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSThinkboxDeadlineSpotEventPluginAdminPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:38 UTC
- Ora modificata: 27 maggio 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DescribeSpotFleetInstances",
```

```
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

Descrizione: concedi le autorizzazioni necessarie per un'istanza EC2 che esegue il software AWS Thinkbox Deadline Spot Event Plugin Worker.

`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 maggio 2020, 19:35 UTC
- Ora modificata: 07 dicembre 2020, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineResourceTracker" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueUrl",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransferConsoleFullAccess

Descrizione: fornisce l'accesso completo a AWS Transfer tramite Console di gestione AWS

`AWSTransferConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSTransferConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 dicembre 2020, 19:33 UTC
- Ora modificata: 14 dicembre 2020, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "health:DescribeEventAggregates",
        "iam:GetPolicyVersion",
        "iam:ListPolicies",
        "iam:ListRoles",
        "route53:ListHostedZones",
        "s3:ListAllMyBuckets",
        "transfer:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransferFullAccess

Descrizione: fornisce l'accesso completo al servizio di AWS trasferimento.

`AWSTransferFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSTransferFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 dicembre 2020, 19:37 UTC
- Ora modificata: 14 dicembre 2020, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "transfer:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransferLoggingAccess

Descrizione: consente a AWS Transfer l'accesso completo per creare flussi e gruppi di log e inserire eventi di registro nel tuo account

`AWSTransferLoggingAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSTransferLoggingAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 gennaio 2019, 15:32 UTC
- Ora modificata: 14 gennaio 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransferReadOnlyAccess

Descrizione: Fornisci l'accesso in sola lettura ai servizi di AWS trasferimento.

`AWSTransferReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSTransferReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 agosto 2020, 17:54 UTC
- Ora modificata: 27 agosto 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransformApplicationDeploymentPolicy

Descrizione: consente al servizio AWS Transform di distribuire applicazioni.NET trasformate creando e gestendo AWS risorse. Questa politica concede le autorizzazioni per il provisioning dell'infrastruttura, la gestione delle risorse di elaborazione e la configurazione delle impostazioni di distribuzione su vari servizi. AWS

`AWSTransformApplicationDeploymentPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSTransformApplicationDeploymentPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 28 agosto 2025, 06:34 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationDeploymentPolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSTransform*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:UpdateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAnyValue:StringNotEquals" : {
          "aws:TagKeys" : [
            "Name",
            "CreatedBy",
            "ApplicationName",
            "TransformationType",
            "aws:cloudformation:stack-name",
            "aws:cloudformation:logical-id",
            "aws:cloudformation:stack-id"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-App-Instance-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/ami-amazon-linux-latest*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunRemoteScript"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:PutBucketTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-transform-deployment-bucket-*",
        "arn:aws:s3:::aws-transform-deployment-bucket-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedFor" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws-transform" : "*",
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ebs:id" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransformApplicationECSDeploymentPolicy

Descrizione: consente a AWS Transform di distribuire applicazioni su Amazon Elastic Container Service (ECS) con Fargate. Concede le autorizzazioni per fornire, configurare e gestire l'infrastruttura sottostante necessaria per eseguire le applicazioni su ECS.

`AWSTransformApplicationECSDeploymentPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSTransformApplicationECSDeploymentPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 29 settembre 2025, 22:49 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationECSDeploymentPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:CreateStack",
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RegisterTaskDefinition",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RunTask",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:ListTasks",
      "Resource" : "arn:aws:ecs:*:*:container-instance/AWSTransform*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:DescribeTasks",
      "Resource" : "arn:aws:ecs:*:*:task/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
```

```
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateService",
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService"
      ],
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:ecs:*:*:cluster/AWSTransform*",
        "arn:aws:ecs:*:*:task-definition/AWSTransform*",
        "arn:aws:ecs:*:*:service/AWSTransform*",
        "arn:aws:ecs:*:*:task/AWSTransform*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:UntagResource",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/awstransform*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
```

```
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ecr.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ecr:arn" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransformCustomExecuteTransformations

Descrizione: fornisce l'accesso per eseguire trasformazioni in AWS Transform custom.

`AWSTransformCustomExecuteTransformations`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSTransformCustomExecuteTransformations` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 dicembre 2025, 15:34 UTC
- Ora modificata: 27 aprile 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomExecuteTransformations`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomExecuteTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:ExecuteTransformation",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/transform-custom.amazonaws.com/
AWSServiceRoleForAWSTransformCustom"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "transform-custom.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransformCustomFullAccess

Descrizione: fornisce l'accesso completo a AWS Transform custom.

`AWSTransformCustomFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSTransformCustomFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 dicembre 2025, 15:19 UTC

- Ora modificata: 07 aprile 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomAllActions",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/transform-custom.amazonaws.com/
AWSServiceRoleForAWSTransformCustom"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "transform-custom.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransformCustomManageTransformations

Descrizione: consente la gestione delle risorse di trasformazione e l'esecuzione delle trasformazioni in AWS Transform custom.

`AWSTransformCustomManageTransformations`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSTransformCustomManageTransformations` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 dicembre 2025, 15:49 UTC
- Ora modificata: 27 aprile 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomManageTransformations`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomManageTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:CreateTransformationPackageUrl",
        "transform-custom:CompleteTransformationPackageUpload",
        "transform-custom:DeleteTransformationPackage",
        "transform-custom:GetTransformationPackageUrl",
        "transform-custom:ListTransformationPackageMetadata",
        "transform-custom:ExecuteTransformation",
        "transform-custom:ListKnowledgeItems",
        "transform-custom:GetKnowledgeItem",
        "transform-custom:DeleteKnowledgeItem",
        "transform-custom:UpdateKnowledgeItemConfiguration",
        "transform-custom:UpdateKnowledgeItemStatus",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign",
        "transform-custom:ListTagsForResource",
        "transform-custom:TagResource",
        "transform-custom:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/transform-custom.amazonaws.com/
AWSServiceRoleForAWSTransformCustom"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "transform-custom.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransformInfrastructureExecutorAccessBatch

Descrizione: concede agli sviluppatori del ruolo di esecuzione le autorizzazioni necessarie per eseguire AWS Transform Continuous Modernization CLI/agent assessments/transformations utilizzando AWS Batch, tra cui il caricamento del codice sorgente, il recupero dei risultati, il monitoraggio dello stato del lavoro Batch, la lettura dei log e la gestione delle pianificazioni di trasformazione.

`AWSTransformInfrastructureExecutorAccessBatch`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AWSTransformInfrastructureExecutorAccessBatch` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 luglio 2026, 20:12 UTC
- Ora modificata: 28 luglio 2026, 15:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformInfrastructureExecutorAccessBatch`

Versione della politica

Versione della politica: v2 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LambdaInvokeATXFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:atx-trigger-job-*",
        "arn:aws:lambda:*:*:function:atx-trigger-batch-jobs-*",
        "arn:aws:lambda:*:*:function:atx-get-job-status-*",
        "arn:aws:lambda:*:*:function:atx-get-batch-status-*",
        "arn:aws:lambda:*:*:function:atx-list-jobs-*",
        "arn:aws:lambda:*:*:function:atx-list-batches-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3UploadSourceCode",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:AbortMultipartUpload"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::atx-source-code-*",
        "arn:aws:s3:::atx-source-code-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3DownloadResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-custom-output-*",
        "arn:aws:s3:::atx-custom-output-*/*",
        "arn:aws:s3:::atx-ct-output-*",
        "arn:aws:s3:::atx-ct-output-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3WriteBatchSidecar",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-custom-output-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "KMSEncryptDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : [
            "alias/atx-encryption-key",
            "alias/atx-encryption-key-*"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchReadLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/batch/atx-transform*",
        "arn:aws:logs:*:*:log-group:/aws/batch/job*",
        "arn:aws:logs:*:*:log-group:AtxVpc*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/atx-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchDashboard",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetDashboard",
        "cloudwatch:ListDashboards"
      ],
      "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/ATX-Transform-CLI-Dashboard",
        "arn:aws:cloudwatch::*:dashboard/ATX-Transform-CLI-Dashboard-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BatchDescribe",
      "Effect" : "Allow",
      "Action" : [
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobs",
        "batch:ListJobs"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CheckInfrastructureStatus",
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AtxInfrastructureStack/*",
        "arn:aws:cloudformation:*:*:stack/AtxInfrastructureStack-*/*",
        "arn:aws:cloudformation:*:*:stack/atx-*",
        "arn:aws:cloudformation:*:*:stack/atx-*/*",
        "arn:aws:cloudformation:*:*:stack/AtxSecurityAgentStack-*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerATXSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedulerManage",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/atx-ct",
        "arn:aws:scheduler:*:*:schedule-group/atx-ct-*",
        "arn:aws:scheduler:*:*:schedule/atx-ct/*",
        "arn:aws:scheduler:*:*:schedule/atx-ct-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassSchedulerRole",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole",
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMReadRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/ATX*",
        "arn:aws:iam::*:role/Atx*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagGetATXStacks",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CFNListStacksForDetect",
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStacks",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransformInfrastructureExecutorAccessEC2

Descrizione: concede al ruolo di esecuzione degli sviluppatori le autorizzazioni necessarie per eseguire AWS Transform Continuous Modernization CLI/agent assessments/transformations

utilizzando EC2, tra cui il caricamento del codice sorgente, il recupero dei risultati, il monitoraggio dello stato del lavoro, la lettura dei registri e la gestione delle pianificazioni di trasformazione.

`AWSTransformInfrastructureExecutorAccessEC2`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AWSTransformInfrastructureExecutorAccessEC2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 luglio 2026, 20:12 UTC
- Ora modificata: 28 luglio 2026, 15:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformInfrastructureExecutorAccessEC2`

Versione della politica

Versione della politica: v2 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CFNRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackDriftDetectionStatus"
      ],
      "Resource" : [
```

```
        "arn:aws:cloudformation:*:*:stack/atx-*/*",
        "arn:aws:cloudformation:*:*:stack/AtxSecurityAgentStack-*/*"
      ]
    },
    {
      "Sid" : "CFNValidateTemplate",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Desc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2PowerState",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/atx-remote-infra" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "SSMRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeSessions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMTgt",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/atx-remote-infra" : "true"
        }
      }
    },
    {
      "Sid" : "SSMDocs",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*::document/AWS-RunShellScript"
    },
    {
      "Sid" : "S3Data",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
```

```
        "s3:DeleteObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-source-code-*",
        "arn:aws:s3:::atx-source-code-*/*",
        "arn:aws:s3:::atx-ct-output-*",
        "arn:aws:s3:::atx-ct-output-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSEncryptDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : [
            "alias/atx-encryption-key",
            "alias/atx-encryption-key-*"
          ]
        }
      }
    },
    {
      "Sid" : "SM",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SMList",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/atx-ct/*",
        "arn:aws:scheduler:*:*:schedule/atx-ct-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedGroupRead",
      "Effect" : "Allow",
      "Action" : "scheduler:GetScheduleGroup",
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/atx-ct",
        "arn:aws:scheduler:*:*:schedule-group/atx-ct-*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedList",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassEC2InstanceRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/atx-transform-role",
        "arn:aws:iam::*:role/atx-transform-role-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassSchedulerRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole",
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole-*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMReadRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/atx-*",
        "arn:aws:iam::*:role/Atx*",
        "arn:aws:iam::*:role/ATX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMReadInstanceProfile",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/atx-*",
        "arn:aws:iam::*:instance-profile/Atx*",
        "arn:aws:iam::*:instance-profile/ATX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagGetATXStacks",
      "Effect" : "Allow",
```

```
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CFNListStacksForDetect",
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStacks",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransformRevenueAttributionPolicy

Descrizione: consente al servizio AWS Transform di gestire l'attribuzione dei ricavi dei clienti per gli incentivi.

`AWSTransformRevenueAttributionPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSTransformRevenueAttributionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 luglio 2026, 16:42 UTC
- Ora modificata: 07 luglio 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformRevenueAttributionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PartnerCentralRevenueManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetRevenueAttribution",
        "partnercentral:UpdateRevenueAttribution",
        "partnercentral:CreateRevenueAttribution",
        "partnercentral:ListRevenueAttributions"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransformSecretsManagerConnectorPolicy

Descrizione: consente al servizio AWS Transform di leggere un SecretsManager segreto specificato in connessione alla chiave KMS specificata. Questa politica concede le autorizzazioni per leggere il valore segreto specificato e decrittografarlo se il segreto è crittografato

`AWSTransformSecretsManagerConnectorPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSTransformSecretsManagerConnectorPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 marzo 2026, 21:12 UTC
- Ora modificata: 4 marzo 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformSecretsManagerConnectorPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadSecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:${aws:PrincipalTag/SecretId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DecryptWithCustomerProvidedKMSKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KMSKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:
${aws:RequestedRegion}:${aws:PrincipalAccount}:secret:${aws:PrincipalTag/SecretId}",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeKMSKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTransformSecurityAgentExecutorAccess

Descrizione: concede a AWS Transform (ATX) Continuous Modernization le autorizzazioni necessarie per richiamare CLI/agent il servizio AWS Security Agent per le revisioni e le correzioni automatiche della sicurezza del codice, incluso il caricamento degli artefatti di scansione e il recupero dei risultati.

`AWSTransformSecurityAgentExecutorAccess`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `AWSTransformSecurityAgentExecutorAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 giugno 2026, 21:27 UTC
- Ora modificata: 28 luglio 2026, 15:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformSecurityAgentExecutorAccess`

Versione della politica

Versione della politica: v2 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityAgentApi",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:CreateCodeReview",
        "securityagent:StartCodeReviewJob",
        "securityagent:ListCodeReviewJobsForCodeReview",
        "securityagent:ListFindings",
        "securityagent:BatchGetFindings",
        "securityagent:StartCodeRemediation"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3SecurityAgentBucketRead",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-security-agent-*",
        "arn:aws:s3:::atx-security-agent-*/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3SecurityAgentUpload",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::atx-security-agent-*/security-scans/*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassSecurityAgentRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/security-agent-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "securityagent.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CFNDiscoverSecurityAgentStack",
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStacks",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CFNDescribeSecurityAgentStack",
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
```

```
      "Resource" : "arn:aws:cloudformation:*:*:stack/AtxSecurityAgentStack-*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTrustedAdvisorPriorityFullAccess

Descrizione: Fornisce l'accesso completo a AWS Trusted Advisor Priority. Questa politica consente inoltre all'utente di aggiungere Trusted Advisor come servizio affidabile con AWS Organizations e di specificare account amministrativi delegati per Trusted Advisor Priority.

`AWSTrustedAdvisorPriorityFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSTrustedAdvisorPriorityFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 agosto 2022, 16:08 UTC
- Ora modificata: 16 agosto 2022, 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:UpdateRiskStatus",
        "trustedadvisor:DescribeNotificationConfigurations",
        "trustedadvisor:UpdateNotificationConfigurations",
        "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
        "trustedadvisor:SetOrganizationAccess"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "reporting.trustedadvisor.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTrustedAdvisorPriorityReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS Trusted Advisor Priority. Ciò include l'autorizzazione a visualizzare gli account degli amministratori delegati.

`AWSTrustedAdvisorPriorityReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSTrustedAdvisorPriorityReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 agosto 2022, 16:35 UTC
- Ora modificata: 16 agosto 2022, 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:DescribeNotificationConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTrustedAdvisorReportingServiceRolePolicy

Descrizione: Politica di servizio per la reportistica su più account di Trusted Advisor

`AWSTrustedAdvisorReportingServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 novembre 2019, 17:41 UTC
- Ora modificata: 28 febbraio 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
```

```
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSTrustedAdvisorServiceRolePolicy

Descrizione: Accesso al servizio AWS Trusted Advisor per ridurre i costi, aumentare le prestazioni e migliorare la sicurezza dell' AWS ambiente.

`AWSTrustedAdvisorServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 22 febbraio 2018, 21:24 UTC
- Ora modificata: 14 maggio 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "dax:DescribeClusters",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
```

```
        "ec2:DescribeImages",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:GetManagedPrefixListEntries",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTaskDefinitions",
        "ecs:ListClusters",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "ecs:ListTaskDefinitionFamilies",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "iam:ListSAMLProviders",
        "kinesis:DescribeLimits",
        "kafka:DescribeClusterV2",
        "kafka:ListClustersV2",
        "kafka:ListNodes",
        "network-firewall:ListFirewalls",
        "network-firewall:DescribeFirewall",
        "outposts:ListAssets",
```

```
        "outposts:GetOutpost",
        "outposts:ListOutposts",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:GetQueueAttributes",
```

```
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSUserAttributeCostAllocationPolicy

Descrizione: fornisce accesso in sola lettura agli attributi utente da AWS IAM Identity Center per gli attributi utente che il cliente ha accettato.

`AWSUserAttributeCostAllocationPolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 dicembre 2025, 16:34 UTC
- Ora modificata: 15 dicembre 2025, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserAttributeCostAllocationPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/user-attribute-cost-
allocation-data.amazonaws.com/AWSServiceRoleForUserAttributeCostAllocation"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSUserNotificationsServiceLinkedRolePolicy

Descrizione: consente alle notifiche AWS utente di chiamare AWS i servizi per tuo conto.

`AWSUserNotificationsServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 aprile 2023, 13:28 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AWSUserNotificationsManagedRule-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Notifications"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrgsActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "notifications.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationNotificationConfigurationDistribution",
      "Effect" : "Allow",
      "Action" : [
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteNotificationConfiguration",
        "notifications:CreateEventRule",
        "notifications:UpdateEventRule",
        "notifications:DeleteEventRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSVendorInsightsAssessorFullAccess

Descrizione: fornisce l'accesso completo alla visualizzazione delle risorse Vendor Insights autorizzate e alla gestione degli abbonamenti Vendor Insights

`AWSVendorInsightsAssessorFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSVendorInsightsAssessorFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 luglio 2022, 15:05 UTC
- Ora modificata: 01 dicembre 2022, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSVendorInsightsAssessorReadOnly

Descrizione: fornisce l'accesso in sola lettura per la visualizzazione delle risorse Vendor Insights autorizzate

`AWSVendorInsightsAssessorReadOnly`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSVendorInsightsAssessorReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 luglio 2022, 15:05 UTC
- Ora modificata: 01 dicembre 2022, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:ListEntitledSecurityProfiles",
```

```
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSVendorInsightsVendorFullAccess

Descrizione: fornisce l'accesso completo per la creazione e la gestione delle risorse di Vendor Insights

`AWSVendorInsightsVendorFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSVendorInsightsVendorFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 luglio 2022, 15:05 UTC

- Ora modificata: 19 ottobre 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:CreateDataSource",
        "vendor-insights:UpdateDataSource",
        "vendor-insights:DeleteDataSource",
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:CreateSecurityProfile",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:AssociateDataSource",
        "vendor-insights:DisassociateDataSource",
        "vendor-insights:UpdateSecurityProfile",
        "vendor-insights:ActivateSecurityProfile",
        "vendor-insights:DeactivateSecurityProfile",
```

```
        "vendor-insights:UpdateSecurityProfileSnapshotCreationConfiguration",
        "vendor-insights:UpdateSecurityProfileSnapshotReleaseConfiguration",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:TagResource",
        "vendor-insights:UntagResource",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:CancelAgreement",
        "aws-marketplace:SearchAgreements"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSVendorInsightsVendorReadOnly

Descrizione: fornisce l'accesso in sola lettura per la visualizzazione delle risorse di Vendor Insights

`AWSVendorInsightsVendorReadOnly`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `AWSVendorInsightsVendorReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 26 luglio 2022, 15:05 UTC
- Ora modificata: 01 dicembre 2022, 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSVPCFlowLogsServiceRolePolicy

Descrizione: fornisce le autorizzazioni per controllare le risorse gestite dal servizio e chiamare le API necessarie per l'arricchimento dei campi di registro per conto dei clienti.

`AWSVPCFlowLogsServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 11 maggio 2026, 15:57 UTC
- Ora modificata: 11 maggio 2026, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCFlowLogsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : [
        "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
        "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.tag",
            "aws.autoscaling"
          ],
          "events:detail-type" : [
            "AWS API Call via CloudTrail",
            "Tag Change on Resource"
          ]
        },
        "Null" : {
          "events:source" : "false",
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByVPCFlowLogs",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
        "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeTagsOnAllEC2Resources",
      "Effect" : "Allow",
      "Action" : [
```

```
        "tag:GetResources",
        "autoscaling:DescribeTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSVpcLatticeServiceRolePolicy

Descrizione: consente a VPC Lattice di accedere alle AWS risorse per tuo conto.

`AWSVpcLatticeServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 30 novembre 2022, 20:47 UTC
- Ora modificata: 01 dicembre 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    },
    {
      "Sid" : "VpcLatticeDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VpcLatticeManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithSubnetAndSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VpcLatticeTagNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "VpcLatticeMutateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceActionsIpAddressActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeAssociateHostedZoneToVpc",
      "Effect" : "Allow",
      "Action" : [
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSVPCS2SVpnServiceRolePolicy

Descrizione: consenti alla Site-to-Site VPN di creare e gestire risorse relative alle tue connessioni VPN.

`AWSVPCS2SVpnServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 6 agosto 2019, 14:13 UTC
- Ora modificata: 15 maggio 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpnConnectionSecretsManagement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "s2svpn",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpnConnectionSecretsCreation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "s2svpn!*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSVPCTransitGatewayServiceRolePolicy

Descrizione: consenti a VPC Transit Gateway di creare e gestire le risorse necessarie per gli allegati VPC Transit Gateway.

`AWSVPCTransitGatewayServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 novembre 2018, 16:21 UTC
- Ora modificata: 15 aprile 2021, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AssignIpv6Addresses",
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Sid" : "0"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSVPCVerifiedAccessServiceRolePolicy

Descrizione: politica per consentire al servizio AWS Verified Access di fornire gli endpoint per tuo conto

`AWSVPCVerifiedAccessServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 29 novembre 2022, 03:35 UTC
- Ora modificata: 17 novembre 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VerifiedAccessRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleModifyNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VerifiedAccessRoleNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VerifiedAccessRoleTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSWAFConsoleFullAccess

Descrizione: Fornisce l'accesso completo a AWS WAF tramite. Console di gestione AWS Tieni presente che questa politica concede anche le autorizzazioni per elencare e aggiornare le CloudFront distribuzioni Amazon, le autorizzazioni per visualizzare i sistemi di bilanciamento del carico su Elastic Load AWS Balancing, le autorizzazioni per visualizzare le API e le fasi REST di Amazon API Gateway, le autorizzazioni per elencare e visualizzare i parametri Amazon e le autorizzazioni per visualizzare le regioni abilitate all' CloudWatch interno dell'account.

`AWSWAFConsoleFullAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSWAFConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 aprile 2020, 18:38 UTC
- Ora modificata: 01 luglio 2026, 04:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Versione della politica

Versione della politica: v22 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
```

```
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
```

```
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
```

```
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant",
        "cloudfront:AssociateDistributionTenantWebACL",
        "cloudfront:DisassociateDistributionTenantWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation",
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
```

```
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL",
        "appsync:AssociateWebACL",
        "appsync:DisassociateWebACL",
        "appsync:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
```

```
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
```

```
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : "pricingplanmanager:ListSubscriptions",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayAssociateWebACL",
        "bedrock-agentcore:GatewayDisassociateWebACL",
        "bedrock-agentcore:GatewayGetWebACLForResource",
        "bedrock-agentcore:GetGateway"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL",
        "bedrock-agentcore:ListGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSWAFConsoleReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS WAF tramite. Console di gestione AWS Tieni presente che questa politica concede anche le autorizzazioni per elencare le CloudFront distribuzioni Amazon, le autorizzazioni per visualizzare i sistemi di bilanciamento del carico su Elastic Load AWS Balancing, le autorizzazioni per visualizzare le API e le fasi REST di Amazon API Gateway, le autorizzazioni per elencare e visualizzare i parametri Amazon e le autorizzazioni per visualizzare le regioni abilitate all' CloudWatch interno dell'account.

`AWSWAFConsoleReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSWAFConsoleReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 aprile 2020, 18:43 UTC
- Ora modificata: 01 luglio 2026, 04:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v21 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
```

```
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
```

```
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFrontTenant",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudfront:GetDistributionTenant"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowGetActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetWebACLForResource"
```

```
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
```

```
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListSubscriptionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ListSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayGetWebACLForResource",
        "bedrock-agentcore:GetGateway"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL",
        "bedrock-agentcore:ListGateways"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSWAFFullAccess

Descrizione: fornisce l'accesso completo alle azioni AWS WAF.

`AWSWAFFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSWAFFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 ottobre 2015, 20:44 UTC
- Ora modificata: 28 luglio 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Versione della politica

Versione della politica: v17 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
```

```
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation",
        "elasticloadbalancing:GetLoadBalancerWebACL"
```

```
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL",
        "appsync:AssociateWebACL",
        "appsync:DisassociateWebACL",
        "appsync:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
```

```
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
```

```
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayAssociateWebACL",
        "bedrock-agentcore:GatewayDisassociateWebACL",
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSWAFReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle azioni AWS WAF.

`AWSWAFReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSWAFReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 ottobre 2015, 20:43 UTC
- Ora modificata: 01 luglio 2026, 04:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Versione della politica

Versione della politica: v13 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
```

```
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
```

```
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListResourcesForWebACL"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSWellArchitectedDiscoveryServiceRolePolicy

Descrizione: consente di accedere WellArchitected a AWS servizi e risorse correlati alle WellArchitected risorse per conto dei clienti.

`AWSWellArchitectedDiscoveryServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 aprile 2023, 18:36 UTC
- Ora modificata: 26 aprile 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
```

```
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:GetApplication",
        "servicecatalog:CreateAttributeGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/applications/*",
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:UpdateAttributeGroup",
```

```
        "servicecatalog:DeleteAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSWellArchitectedOrganizationsServiceRolePolicy

Descrizione: consente a Well-Architected di accedere a Organizations per tuo conto.

`AWSWellArchitectedOrganizationsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 23 giugno 2022, 17:15 UTC
- Ora modificata: 25 luglio 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSWickrFullAccess

Descrizione: Questa politica concede autorizzazioni amministrative complete al servizio Wickr, comprese le funzioni amministrative di Wickr ai sensi del. Console di gestione AWS

`AWSWickrFullAccess`AWS è una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSWickrFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 20:36 UTC
- Ora modificata: 27 novembre 2022, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSXrayCrossAccountSharingConfiguration

Descrizione: Fornisce funzionalità per gestire i collegamenti di Observability Access Manager e stabilire la condivisione di tracce a raggi X

`AWSXrayCrossAccountSharingConfiguration`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSXrayCrossAccountSharingConfiguration` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 13:46 UTC
- Ora modificata: 27 novembre 2022, 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:Link",
        "oam:ListLinks"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSXRayDaemonWriteAccess

Descrizione: consente al demone AWS X-Ray di inoltrare i dati grezzi dei segmenti di traccia all'API del servizio e di recuperare i dati di campionamento (regole, obiettivi, ecc.) da utilizzare con X-Ray SDK.

`AWSXRayDaemonWriteAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `AWSXRayDaemonWriteAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 agosto 2018, 23:00 UTC
- Ora modificata: 13 febbraio 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSXrayFullAccess

Descrizione: policy di accesso completo AWS gestito a X-Ray

`AWSXrayFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSXrayFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2016, 18:30 UTC
- Ora modificata: 11 aprile 2024, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSXrayReadOnlyAccess

Descrizione: policy gestita in modalità di sola lettura AWS X-Ray

`AWSXrayReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSXrayReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2016, 18:27 UTC
- Ora modificata: 14 febbraio 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries",
        "xray:BatchGetTraces",
        "xray:BatchGetTraceSummaryById",
        "xray:GetDistinctTraceGraphs",
        "xray:GetServiceGraph",
        "xray:GetTraceGraph",
        "xray:GetTraceSummaries",
        "xray:GetGroups",
        "xray:GetGroup",
        "xray:ListTagsForResource",
        "xray:ListResourcePolicies",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetInsightSummaries",
        "xray:GetInsight",
        "xray:GetInsightEvents",
        "xray:GetInsightImpactGraph"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSXrayWriteOnlyAccess

Descrizione: policy AWS gestita solo in scrittura X-Ray

`AWSXrayWriteOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `AWSXrayWriteOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2016, 18:19 UTC
- Ora modificata: 28 agosto 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSZonalAutoshiftPracticeRunSLRPolicy

Descrizione: fornisce l'accesso amministrativo per le esercitazioni dei turni zonali ARC e l'accesso agli stati degli CloudWatch allarmi per monitorare gli allenamenti.

`AWSZonalAutoshiftPracticeRunSLRPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 29 novembre 2023, 17:34 UTC

- Ora modificata: 30 giugno 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoshiftPracticeCheckPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ZonalShiftManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "arc-zonal-shift:CancelZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:UpdateZonalShift"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

AWSZoneGroupAccessManagementServiceRolePolicy

Descrizione: fornisce accesso in sola lettura a quanto APIs necessario per supportare la gestione degli accessi in gruppi di zone per le organizzazioni.

`AWSZoneGroupAccessManagementServiceRolePolicy`è AWS una politica gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 1 luglio 2025, 19:07 UTC
- Ora modificata: 01 luglio 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZoneGroupAccessManagementServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

BatchServiceRolePolicy

Descrizione: fornisce l'accesso al servizio AWS Batch per gestire le risorse richieste, incluse le risorse Amazon EC2 e Amazon ECS.

`BatchServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 marzo 2021, 06:55 UTC
- Ora modificata: 05 dicembre 2023, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
```

```
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RequestSpotFleet",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "eks:DescribeCluster",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:DeregisterTaskDefinition",
        "ecs:TagResource",
        "ecs:ListAccountSettings",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*:log-stream:*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement6",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
```

```
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement9",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteLaunchConfiguration"
      ],
      "Resource" :
  "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/AWSBatch*"
    },
```

```
    {
      "Sid" : "AWSBatchPolicyStatement10",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement11",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement12",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task-definition/*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement13",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
```

```
    },
    {
      "Sid" : "AWSBatchPolicyStatement14",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement15",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:elastic-gpu/*",
        "arn:aws:elastic-inference:*:*:elastic-inference-accelerator/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "AWSBatchPolicyStatement16",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "RequestSpotFleet"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

BedrockAgentCoreFullAccess

Descrizione: fornisce un accesso completo a Bedrock AgentCore e un accesso limitato ai servizi correlati

`BedrockAgentCoreFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `BedrockAgentCoreFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 luglio 2025, 13:37 UTC
- Ora modificata: 28 luglio 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreFullAccess`

Versione della politica

Versione della politica: v18 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAgentCoreFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:*"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:*"
    },
    {
      "Sid" : "IAMListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
```

```
    {
      "Sid" : "BedrockAgentCorePassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*BedrockAgentCore*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:bedrock-agentcore*"
    },
    {
      "Sid" : "BedrockAgentCoreKMSReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
```

```
        "kms:ListGrants"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "bedrock-agentcore.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSGrantsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "bedrock-agentcore.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:bedrock-agentcore-gateway:arn" : "arn:aws:bedrock-
agentcore:*:*:gateway/*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "BedrockAgentCoreS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-gateway-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-agentcore.amazonaws.com",
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreGatewayLambdaAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:*"
      ]
    },
    {
      "Sid" : "BedrockAgentCoreGatewayApiGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*/stages/*/exports/*"
      ]
    },
    {
      "Sid" : "LoggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
```

```
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "ObservabilityReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "oam:ListSinks",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval",
        "logs:DescribeLogGroups",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchXRayPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSegmentDestination",
        "xray:UpdateTraceSegmentDestination",
        "xray:GetIndexingRules",
        "xray:UpdateIndexingRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "TransactionSearchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TransactionSearchApplicationSignalsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:StartDiscovery"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CreateBedrockAgentCoreNetworkServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/network.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreNetwork",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBedrockAgentCoreGatewayNetworkServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreGatewayNetwork",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "bedrock-agentcore.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "CreateBedrockAgentCoreRuntimeIdentityServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/runtime-identity.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreRuntimeIdentity",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "runtime-identity.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3WriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-runtime-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeECRAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:DescribeImages",
        "ecr:ListImages"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/evaluations/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogIndexAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutIndexPolicy",
        "logs:DescribeIndexPolicies"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/spans",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockInvokeAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationLambdaAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:GetFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*"
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockMantleInference",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CreateInference",
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CallWithBearerToken",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

BedrockAgentCoreNetworkServiceRolePolicy

Descrizione: consente l'accesso ad altre risorse di AWS servizio necessarie per eseguire Amazon Bedrock AgentCore in modalità VPC

`BedrockAgentCoreNetworkServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 settembre 2025, 22:04 UTC
- Ora modificata: 19 settembre 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreNetworkServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateEniInAnySubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Sid" : "AllowCreateEniWithSecurityGroups",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "AllowCreateEniWithBedrockManagedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonBedrockAgentCoreManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowTagEniOnCreate",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "AllowManageEniWhenBedrockManaged",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowGetSecurityGroupsForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetSecurityGroupsForVPC"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "AllowDescribeNetworkingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

BedrockAgentCoreRuntimeIdentityServiceRolePolicy

Descrizione: consente l'accesso alle risorse di gestione delle identità e dei token necessarie per l'autenticazione e l'autorizzazione di Amazon Bedrock AgentCore Runtime.

`BedrockAgentCoreRuntimeIdentityServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 11 ottobre 2025, 01:04 UTC
- Ora modificata: 11 ottobre 2025, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreRuntimeIdentityServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Sid" : "AllowWorkloadIdentityAccess",
    "Effect" : "Allow",
    "Action" : [
      "bedrock-agentcore:GetWorkloadAccessToken",
      "bedrock-agentcore:GetWorkloadAccessTokenForJWT",
      "bedrock-agentcore:GetWorkloadAccessTokenForUserId"
    ],
    "Resource" : [
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default",
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default/workload-
identity/*"
    ]
  }
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

Fatturazione

Descrizione: concede le autorizzazioni per la fatturazione e la gestione dei costi. Ciò include la visualizzazione dell'utilizzo dell'account e la visualizzazione e modifica dei budget e dei metodi di pagamento.

`Billing`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `Billing` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica relativa alle funzioni lavorative

- Ora di creazione: 10 novembre 2016, 17:33 UTC
- Ora modificata: 30 luglio 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Versione della politica

Versione della politica: v30 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:CreateBillingView",
        "billing:DeleteBillingView",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:GetResourcePolicy",
        "billing:ListSourceViewsForBillingView",
```

```
        "billing:ListTagsForResource",
        "billing:TagResource",
        "billing:UntagResource",
        "billing:UpdateBillingPreferences",
        "billing:UpdateBillingView",
        "billing:UpdateIAMAccessPreference",
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "budgets:ExecuteBudgetAction",
        "budgets:ModifyBudget",
        "budgets:UpdateBudgetAction",
        "budgets:ViewBudget",
        "ce:CreateCostCategoryDefinition",
        "ce:CreateNotificationSubscription",
        "ce:CreateReport",
        "ce:DeleteCostCategoryDefinition",
        "ce:DeleteNotificationSubscription",
        "ce:DeleteReport",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListCostCategoryResourceAssociations",
        "ce:ListTagsForResource",
        "ce:TagResource",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:UpdateNotificationSubscription",
        "ce:UpdatePreferences",
        "ce:UpdateReport",
        "ce:UpdateCostCategoryDefinition",
        "ce:UntagResource",
        "ce:StartCostAllocationTagBackfill",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions",
        "cur:GetClassicReport",
```

```
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:ModifyReportDefinition",
        "cur:PutClassicReportPreferences",
        "cur:PutReportDefinition",
        "cur:ValidateReportDestination",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:PutFreeTierAlertPreference",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:CreateInvoiceUnit",
        "invoicing:DeleteInvoiceUnit",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:ListProcurementPortals",
        "invoicing:ListProcurementPortalSuppliers",
        "invoicing:CreateProcurementPortalPreference",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:PutProcurementPortalPreference",
        "invoicing:UpdateProcurementPortalPreferenceStatus",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:DeleteProcurementPortalPreference",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "invoicing:StartInvoiceCorrection",
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "invoicing:SendProcurementPortalValidation",
        "invoicing:TagResource",
        "invoicing:UntagResource",
        "invoicing:UpdateInvoiceUnit",
        "invoicing:VerifyProcurementPortalValidation",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:CreateFinancingApplication",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
```

```
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "payments:ListPaymentInstruments",
        "payments:MakePayment",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:UpdateFinancingApplication",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences",
        "pricing:DescribeServices",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "support:CreateCase",
        "support:AddAttachmentsToSet",
        "sustainability:GetCarbonFootprintSummary",
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxInheritance",
        "tax:PutTaxInterview",
        "tax:PutTaxRegistration",
```

```
        "tax:UpdateExemptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

BudgetsServiceRolePolicy

Descrizione: consente a Budgets di verificare l'accesso alle visualizzazioni di fatturazione condivise oltre i confini dell'account.

`BudgetsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 30 luglio 2025, 21:07 UTC
- Ora modificata: 30 luglio 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BudgetsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetBillingViewData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CertificateManagerServiceRolePolicy

Descrizione: Politica sul ruolo del servizio Amazon Certificate Manager

`CertificateManagerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 25 giugno 2020, 17:56 UTC

- Ora modificata: 25 giugno 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ClientVPNServiceConnectionsRolePolicy

Descrizione: Politica per consentire a AWS Client VPN di gestire le connessioni degli endpoint Client VPN.

`ClientVPNServiceConnectionsRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 agosto 2020, 19:48 UTC
- Ora modificata: 12 agosto 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ClientVPNServiceRolePolicy

Descrizione: Politica per consentire a AWS Client VPN di gestire gli endpoint Client VPN.

`ClientVPNServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 dicembre 2018, 21:20 UTC
- Ora modificata: 12 agosto 2020, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInternetGateways",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAccountAttributes",
        "ds:AuthorizeApplication",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:UnauthorizeApplication",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "acm:GetCertificate",
        "acm:DescribeCertificate",
        "iam:GetSAMLProvider",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudFormationStackSetsOrgAdminServiceRolePolicy

Descrizione: Ruolo di servizio per CloudFormation StackSets (Organization Master Account)

`CloudFormationStackSetsOrgAdminServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 dicembre 2019, 00:20 UTC
- Ora modificata: 10 dicembre 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsAWSOrganizationsReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "organizations:List*",
        "organizations:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRoleInMemberAccounts",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/stacksets-exec-*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudFormationStackSetsOrgMemberServiceRolePolicy

Descrizione: Ruolo di servizio per CloudFormation StackSets (Account membro dell'organizzazione)

`CloudFormationStackSetsOrgMemberServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 09 dicembre 2019, 23:52 UTC
- Ora modificata: 22 luglio 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Versione della politica

Versione della politica: v2 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stacksets-exec-role-stack-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AdministratorAccess"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudFrontFullAccess

Descrizione: fornisce l'accesso completo alla CloudFront console oltre alla possibilità di elencare i bucket Amazon S3 tramite. Console di gestione AWS

`CloudFrontFullAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudFrontFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 30 luglio 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Versione della politica

Versione della politica: v15 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cffullaccess",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "wafv2:CreateWebACL",
        "kinesis:ListStreams",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:CreateSubscription",
        "cloudwatch:GetMetricData",
        "freetier:GetAccountPlanState",
        "shield:ListProtections"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "cfrequestcertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "cloudfront.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cffdescribestream",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:*"
    },
    {
      "Sid" : "ppmFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ApprovePaidSubscription",
        "pricingplanmanager:AssociateResourcesToSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange",
        "pricingplanmanager:DisassociateResourcesFromSubscription",
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudFrontReadOnlyAccess

Descrizione: fornisce l'accesso alle informazioni sulla configurazione CloudFront della distribuzione e alle distribuzioni degli elenchi tramite. Console di gestione AWS

`CloudFrontReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudFrontReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "iam:ListServerCertificates",
        "route53:List*",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudHSMServiceRolePolicy

Descrizione: consente l'accesso alle AWS risorse utilizzate o gestite da CloudHSM

`CloudHSMServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 6 novembre 2017, 19:12 UTC
- Ora modificata: 6 novembre 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudSearchFullAccess

Descrizione: fornisce l'accesso completo al servizio CloudSearch di configurazione Amazon.

`CloudSearchFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudSearchFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 6 febbraio 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudSearchReadOnlyAccess

Descrizione: fornisce accesso in sola lettura al servizio di CloudSearch configurazione Amazon.

`CloudSearchReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudSearchReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 6 febbraio 2015, 18:39 UTC

- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudTrailEventContext

Descrizione: questo ruolo collegato al servizio consente di CloudTrail ottenere e aggiungere tag di risorse agli CloudTrail eventi del proprietario della risorsa.

`CloudTrailEventContext`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 maggio 2025, 13:52 UTC
- Ora modificata: 15 maggio 2025, 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailEventContext`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventContextPermissionForTag",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleCreation",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
```

```
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.tag"
        },
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:detail-type" : "Tag Change on Resource",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleWrite",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleRead",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*"
    },
    {
      "Sid" : "AllowEventBridgeRuleList",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudTrailServiceRolePolicy

Descrizione: politica di autorizzazione per CloudTrail ServiceLinkedRole

`CloudTrailServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 24 ottobre 2018, 21:21 UTC
- Ora modificata: 27 novembre 2023, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsDelegatedAdminAccess",
      "Effect" : "Allow",
      "Action" : "organizations:ListDelegatedAdministrators",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "DeleteTableAccess",
      "Effect" : "Allow",
      "Action" : "glue:DeleteTable",
      "Resource" : [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/aws:cloudtrail",
        "arn:*:glue:*:*:table/aws:cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeregisterResourceAccess",
      "Effect" : "Allow",
      "Action" : "lakeformation:DeregisterResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatch-CrossAccountAccess

Descrizione: consente di CloudWatch assumere CloudWatch CrossAccountSharing ruoli in account remoti per conto dell'account corrente al fine di visualizzare i dati tra account diversi e tra regioni

`CloudWatch-CrossAccountAccess`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 23 luglio 2019, 09:59 UTC
- Ora modificata: 23 luglio 2019, 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchActionsEC2Access

Descrizione: fornisce accesso in sola lettura ad CloudWatch allarmi e metriche, nonché ai metadati EC2. Fornisce l'accesso alle istanze di Stop, Terminate e Reboot EC2.

`CloudWatchActionsEC2Access`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `CloudWatchActionsEC2Access` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 luglio 2015, 00:00 UTC
- Ora modificata: 07 luglio 2015, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchAgentAdminPolicy

Descrizione: per l'utilizzo AmazonCloudWatchAgent sono necessarie autorizzazioni complete.

`CloudWatchAgentAdminPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchAgentAdminPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 marzo 2018, 00:52 UTC
- Ora modificata: 05 febbraio 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchAgentServerPolicy

Descrizione: autorizzazioni necessarie per l'utilizzo AmazonCloudWatchAgent sui server

`CloudWatchAgentServerPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchAgentServerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 marzo 2018, 01:06 UTC
- Ora modificata: 6 febbraio 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeVolumes",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchAPIKeyAccess

Descrizione: concede le autorizzazioni per effettuare chiamate CloudWatch utilizzando l'autenticazione tramite chiave API.

`CloudWatchAPIKeyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchAPIKeyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 maggio 2026, 08:57 UTC
- Ora modificata: 04 giugno 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAPIKeyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchMetricsAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:CallWithBearerToken",
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "KMSDecryptForCMKDatasets",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "cloudwatch.*.amazonaws.com",
          "kms:EncryptionContext:aws:cloudwatch:arn" : "arn:aws:cloudwatch:*:*:dataset/
*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchApplicationInsightsFullAccess

Descrizione: fornisce l'accesso completo ad CloudWatch Application Insights e alle dipendenze richieste.

`CloudWatchApplicationInsightsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchApplicationInsightsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 24 novembre 2020, 18:44 UTC
- Ora modificata: 25 gennaio 2022, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "sqs:ListQueues",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "autoscaling:DescribeAutoScalingGroups",
        "lambda:ListFunctions",
        "dynamodb:ListTables",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "states:ListStateMachines",
        "apigateway:GET",
        "ecs:ListClusters",
```

```
        "ecs:DescribeTaskDefinition",
        "ecs:ListServices",
        "ecs:ListTasks",
        "eks:ListClusters",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchApplicationInsightsReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad CloudWatch Application Insights.

`CloudWatchApplicationInsightsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchApplicationInsightsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 novembre 2020, 18:48 UTC
- Ora modificata: 24 novembre 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudwatchApplicationInsightsServiceLinkedRolePolicy

Descrizione: policy sui ruoli collegati del servizio Cloudwatch Application Insights

`CloudwatchApplicationInsightsServiceLinkedRolePolicy`è una policy AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 1 dicembre 2018, 16:22 UTC
- Ora modificata: 25 luglio 2024, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v25 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatch",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch:DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:CreateStack",
```

```
        "cloudFormation:UpdateStack",
        "cloudFormation:DeleteStack",
        "cloudFormation:DescribeStackResources",
        "cloudFormation:UpdateTerminationProtection"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "CloudFormationStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:DescribeStacks",
        "cloudFormation:ListStackResources",
        "cloudFormation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ResourceGroups",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "ApplicationInsightsResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "ElasticLoadBalancing",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
    },
```

```
    {
      "Sid" : "SSMAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Sid" : "SSMOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:CreateOpsItem",
        "ssm:DescribeOpsItems",
        "ssm:UpdateOpsItem",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMTags",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "SSMGetCommandInvocation",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-CheckPerformanceCounterSets",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AWSEC2-DetectWorkload",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "Lambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridgeManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "XRay",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetTraceGraph"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:ListTables",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "States",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:DescribeExecution",
        "states:DescribeStateMachine",
        "states:GetExecutionHistory"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "APIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTasks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECSCluster",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateClusterSettings"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "EKS",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
```

```
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:GetSMSAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsDeleteSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
```

```
    {
      "Sid" : "CloudWatchLogsCreateSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*",
        "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
      ]
    },
    {
      "Sid" : "EFS",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:ListHealthChecks",
        "route53:ListQueryLoggingConfigs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53Resolver",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
```

```
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetFirewallRuleGroupAssociation"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchApplicationSignalsFullAccess

Descrizione: Fornisci l'accesso completo al servizio CloudWatch Application Signals e l'accesso mirato alle dipendenze necessarie per utilizzare e gestire questo servizio.

`CloudWatchApplicationSignalsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchApplicationSignalsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 giugno 2024, 22:50 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : "application-signals:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchCreateRumMetricDefinitions",
        "rum:BatchDeleteRumMetricDefinitions",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:PutRumMetricsDestination",
        "rum:UpdateRumMetricDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsPutMetricAlarmPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:SLO-AttainmentGoalAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLO-WarningAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLI-HealthAlarm-*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe"
```

```
      ],
      "Resource" : "arn:aws:sns:*:*:cloudwatch-application-signals-*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsReadPermissions",
      "Effect" : "Allow",
      "Action" : "sns:ListTopics",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
```

```
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchApplicationSignalsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura al servizio CloudWatch Application Signals e l'accesso mirato alle dipendenze necessarie per utilizzare questo servizio

`CloudWatchApplicationSignalsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchApplicationSignalsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 giugno 2024, 22:48 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "application-signals:ListServiceStates",
        "application-signals:ListAuditFindings",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListEntityEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchApplicationSignalsServiceRolePolicy

Descrizione: la politica concede l'autorizzazione ad CloudWatch Application Signals di raccogliere dati di monitoraggio e etichettatura da altri servizi pertinenti AWS .

`CloudWatchApplicationSignalsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 09 novembre 2023, 18:09 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWLogsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "CWListMetricsPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWGetMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ApplicationSignalsPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:GetServiceLevelObjective"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2AutoScalingPermission",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudTrailServiceLinkedChannelCreationPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-signals/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchAutomaticDashboardsAccess

Descrizione: fornisce l'accesso ai dashboard CloudWatch automatici non CloudWatch APIs utilizzati per visualizzare, incluso il contenuto di oggetti come le funzioni Lambda

`CloudWatchAutomaticDashboardsAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchAutomaticDashboardsAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 luglio 2019, 10:01 UTC
- Ora modificata: 20 aprile 2021, 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "elasticache:DescribeCacheClusters",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "lambda:GetFunction",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "synthetics:DescribeCanariesLastRun",
        "tag:GetResources"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchCrossAccountSharingConfiguration

Descrizione: fornisce funzionalità per gestire i collegamenti di Observability Access Manager e stabilire la condivisione delle CloudWatch risorse

`CloudWatchCrossAccountSharingConfiguration`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchCrossAccountSharingConfiguration` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 14:01 UTC
- Ora modificata: 27 novembre 2022, 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchEventsBuiltInTargetExecutionAccess

Descrizione: consente ai target integrati in Amazon CloudWatch Events di eseguire azioni EC2 per tuo conto.

`CloudWatchEventsBuiltInTargetExecutionAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchEventsBuiltInTargetExecutionAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 gennaio 2016, 18:35 UTC
- Ora modificata: 14 gennaio 2016, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchEventsFullAccess

Descrizione: fornisce l'accesso completo ad Amazon CloudWatch Events.

`CloudWatchEventsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchEventsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 14 gennaio 2016, 18:37 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleForCloudWatchEvents",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS_Events_Invoke_Targets"
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchEventsInvocationAccess

Descrizione: consente ad Amazon CloudWatch Events di inoltrare gli eventi agli stream in AWS Kinesis Streams del tuo account.

`CloudWatchEventsInvocationAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `CloudWatchEventsInvocationAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 gennaio 2016, 18:36 UTC
- Ora modificata: 14 gennaio 2016, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchEventsReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon CloudWatch Events.

`CloudWatchEventsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchEventsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 14 gennaio 2016, 18:27 UTC
- Ora modificata: 01 dicembre 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
```

```
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchEventsServiceRolePolicy

Descrizione: consente di AWS CloudWatch eseguire azioni per conto dell'utente configurate tramite allarmi ed eventi.

`CloudWatchEventsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 novembre 2017, 00:42 UTC
- Ora modificata: 17 novembre 2017, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchFullAccess

Descrizione: Fornisce accesso completo a CloudWatch.

`CloudWatchFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 27 novembre 2022, 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudwatch:*",
        "logs:*",
        "sns:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchFullAccessV2

Descrizione: Fornisce accesso completo a CloudWatch.

`CloudWatchFullAccessV2`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchFullAccessV2` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 agosto 2023, 11:32 UTC
- Ora modificata: 08 giugno 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Versione della politica

Versione della politica: v16 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:*",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:CreateCentralizationRuleForOrganization",
        "observabilityadmin:UpdateCentralizationRuleForOrganization",
        "observabilityadmin:DeleteCentralizationRuleForOrganization",
        "observabilityadmin:StartTelemetryEvaluation",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:StopTelemetryEvaluation",
        "observabilityadmin:StartTelemetryEvaluationForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:StopTelemetryEvaluationForOrganization",
        "observabilityadmin:CreateTelemetryRule",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:UpdateTelemetryRule",
        "observabilityadmin:DeleteTelemetryRule",
        "observabilityadmin:CreateTelemetryRuleForOrganization",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:UpdateTelemetryRuleForOrganization",
        "observabilityadmin:DeleteTelemetryRuleForOrganization",
```

```
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:StartTelemetryEnrichment",
        "observabilityadmin:StopTelemetryEnrichment",
        "observabilityadmin:TagResource",
        "observabilityadmin:UntagResource",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:CreateTelemetryPipeline",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:UpdateTelemetryPipeline",
        "observabilityadmin:DeleteTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:CreateS3TableIntegration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:DeleteS3TableIntegration",
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventsServicePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
```

```
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "logs.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" :
 "arn:aws:observabilityadmin:*:*:s3tableintegration/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "logs.amazonaws.com",
            "telemetry-pipelines.observabilityadmin.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:observabilityadmin:*:*:telemetry-
pipeline/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "observabilityadmin.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3tables:PutTableBucketPolicy"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
    },
    {
      "Sid" : "LogAlarmScheduledQueryPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "logs.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:logs:*:*:scheduled-query:*"
        }
      }
    },
    {
      "Sid" : "LogAlarmLogLinesPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudwatch.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudwatch:*:*:alarm:*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchInternetMonitorFullAccess

Descrizione: fornisce l'accesso completo alle azioni per lavorare con Amazon CloudWatch Internet Monitor. Fornisce inoltre l'accesso ad altri servizi, come Amazon CloudWatch, Amazon EC2, CloudFront Amazon ed Elastic Load Balancing WorkSpaces, necessari per utilizzare il servizio Internet Monitor per il monitoraggio e l'archiviazione delle informazioni sul traffico delle applicazioni.

`CloudWatchInternetMonitorFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchInternetMonitorFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 ottobre 2024, 21:02 UTC
- Ora modificata: 22 ottobre 2024, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessActions",
      "Effect" : "Allow",
      "Action" : [
        "internetmonitor:CreateMonitor",
        "internetmonitor:DeleteMonitor",
        "internetmonitor:GetHealthEvent",
```

```
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:Link",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "internetmonitor:TagResource",
        "internetmonitor:UntagResource",
        "internetmonitor:UpdateMonitor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceLinkedRoleActions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "internetmonitor.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RolePolicyActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/aws-service-role/
CloudWatchInternetMonitorServiceRolePolicy"
        }
      }
    },
```

```
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchInternetMonitorReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle azioni per lavorare con Amazon CloudWatch Internet Monitor. Fornisce inoltre l'accesso ad altri servizi in Amazon CloudWatch, comprese le politiche per recuperare informazioni sui CloudWatch parametri e gestire le query di registro, necessarie per utilizzare il servizio Internet Monitor per il monitoraggio e l'archiviazione delle informazioni sul traffico delle applicazioni.

`CloudWatchInternetMonitorReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `CloudWatchInternetMonitorReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 novembre 2024, 23:11 UTC
- Ora modificata: 12 novembre 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
```

```
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchInternetMonitorServiceRolePolicy

Descrizione: consente a Internet Monitor di accedere a EC2, agli spazi di lavoro, CloudFront alle risorse e ad altri servizi richiesti per tuo conto.

`CloudWatchInternetMonitorServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 27 novembre 2022, 17:46 UTC
- Ora modificata: 20 luglio 2023, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
```

```
          "cloudwatch:namespace" : "AWS/InternetMonitor"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchLambdaApplicationSignalsExecutionRolePolicy

Descrizione: fornisce l'accesso in scrittura al gruppo di log X-Ray e CloudWatch Application Signals.

`CloudWatchLambdaApplicationSignalsExecutionRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchLambdaApplicationSignalsExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 ottobre 2024, 19:09 UTC
- Ora modificata: 16 ottobre 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaApplicationSignalsExecutionRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsXrayWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchLambdaInsightsExecutionRolePolicy

Descrizione: policy richiesta per l'estensione Lambda Insights

`CloudWatchLambdaInsightsExecutionRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchLambdaInsightsExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 ottobre 2020, 19:27 UTC
- Ora modificata: 07 ottobre 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda-insights:*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchLogsAPIKeyAccess

Descrizione: concede le autorizzazioni per chiamare CloudWatch i registri utilizzando l'autenticazione con chiave API.

`CloudWatchLogsAPIKeyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `CloudWatchLogsAPIKeyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 febbraio 2026, 19:42 UTC

- Ora modificata: 20 febbraio 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsAPIKeyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogsAPIs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CallWithBearerToken",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSAPIs",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "logs.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:logs:arn" : "arn:aws:logs:*:*:log-group:*"
        }
      },
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
```

```
    {
      "Sid" : "KMSDescribeAPIs",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "logs.*.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchLogsCrossAccountSharingConfiguration

Descrizione: fornisce funzionalità per gestire i collegamenti di Observability Access Manager e stabilire la condivisione delle risorse dei CloudWatch log

`CloudWatchLogsCrossAccountSharingConfiguration`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchLogsCrossAccountSharingConfiguration` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 13:55 UTC

- Ora modificata: 27 novembre 2022, 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
```

```
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchLogsFullAccess

Descrizione: fornisce l'accesso completo ai CloudWatch registri

`CloudWatchLogsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchLogsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchLogsReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura ai CloudWatch registri

`CloudWatchLogsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchLogsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchNetworkFlowMonitorAgentPublishPolicy

Descrizione: puoi utilizzare questa policy nei ruoli IAM collegati alle risorse delle istanze Amazon EC2 e Amazon EKS per inviare report di telemetria (metriche) a un endpoint Network Flow Monitor.

`CloudWatchNetworkFlowMonitorAgentPublishPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `CloudWatchNetworkFlowMonitorAgentPublishPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 dicembre 2024, 22:51 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchNetworkFlowMonitorAgentPublishPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkflowmonitor:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchNetworkFlowMonitorServiceRolePolicy

Descrizione: non puoi collegarti CloudWatchNetworkFlowMonitorServiceRolePolicy alle tue entità IAM. Questa policy è associata a un ruolo collegato al servizio denominato AWSServiceRoleForNetworkFlowMonitor, che pubblica i risultati dell'aggregazione della telemetria di rete, raccolti dagli agenti di Network Flow Monitor, su. CloudWatch Consente inoltre al servizio di utilizzare AWS Organizations per ottenere informazioni per scenari multi-account.

`CloudWatchNetworkFlowMonitorServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 1 dicembre 2024, 22:36 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkFlowMonitor"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

Descrizione: non puoi collegarti CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy alle tue entità IAM. Questa policy è associata a un ruolo collegato al servizio denominato AWSServiceRoleForNetworkFlowMonitor_Topology, che genera istantanee della topologia delle risorse utilizzate da Network Flow Monitor nel tuo account.

`CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 1 dicembre 2024, 22:51 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeCustomerGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PrefixListStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCEndpointStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchNetworkMonitorServiceRolePolicy

Descrizione: consente a CloudWatch Network Monitor di accedere e gestire le risorse EC2 e VPC, pubblicare dati e accedere CloudWatch ad altri servizi richiesti per tuo conto.

`CloudWatchNetworkMonitorServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 21 dicembre 2023, 18:53 UTC
- Ora modificata: 12 dicembre 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCw",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkMonitor"
        }
      }
    },
    {
      "Sid" : "DescribeAny",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayAttachments",
```

```
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteModifyEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchOpenSearchDashboardAccess

Descrizione: questo criterio fornisce agli utenti l'accesso alla visualizzazione dei OpenSearch dashboard sulla console CloudWatch Logs.

`CloudWatchOpenSearchDashboardAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchOpenSearchDashboardAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2024, 21:06 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDirectQueryStatusAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchOpenSearchDashboardsFullAccess

Descrizione: questo criterio fornisce agli utenti l'accesso OpenSearch per creare, aggiornare, eliminare o visualizzare i dashboard nella console CloudWatch Logs.

`CloudWatchOpenSearchDashboardsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchOpenSearchDashboardsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2024, 21:06 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardsFullAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DeleteIntegration",
        "logs:PutIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsOpensearchCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsObservabilityCreateServiceLinkedAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:CreateApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/OpenSearchIntegration" : [
            "Dashboards"
```

```
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:DeleteCollection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:UpdateApplication",
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aoss:CreateSecurityPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsIndexPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:CreateLifecyclePolicy",
        "aoss:DeleteLifecyclePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:index" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSRequestQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsStartDirectQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:StartDirectQuery",
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource",
        "es:DeleteDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "directquery.opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAossTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:TagResource"
      ],
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsApplicationTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:application/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsDataSourceTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a CloudWatch.

`CloudWatchReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Versione della politica

Versione della politica: v24 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudtrail:ListChannels",
```

```
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
```

```
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchReadOnlyGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
```

```
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchSyntheticsFullAccess

Descrizione: Fornisce accesso completo a CloudWatch Synthetics.

`CloudWatchSyntheticsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchSyntheticsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 25 novembre 2019, 17:39 UTC
- Ora modificata: 31 marzo 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Versione della politica

Versione della politica: v14 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*/exports/swagger",
        "arn:aws:apigateway:*::/apis"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::cw-syn-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "synthetics.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogRecord",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:GetLogGroupFields"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/cwsyn-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:cwsyn-*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "lambda:GetLayerVersion",
        "lambda:PublishLayerVersion",
        "lambda:DeleteLayerVersion"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:cwsyn-*",
        "arn:aws:lambda:*:*:layer:Synthetics:*",
        "arn:aws:lambda:*:*:layer:Synthetics_Selenium:*",
        "arn:aws:lambda:*:*:layer:AWS-CW-Synthetics*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Synthetics-*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CloudWatchSyntheticsReadOnlyAccess

Descrizione: Fornisce accesso in sola lettura a CloudWatch Synthetics.

`CloudWatchSyntheticsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CloudWatchSyntheticsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 novembre 2019, 17:45 UTC
- Ora modificata: 6 marzo 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ComprehendDataAccessRolePolicy

Descrizione: Policy for AWS Comprehend service role che consente l'accesso alle risorse S3 per l'accesso ai dati

`ComprehendDataAccessRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ComprehendDataAccessRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 marzo 2019, 22:28 UTC
- Ora modificata: 6 marzo 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ComprehendFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Comprehend.

`ComprehendFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ComprehendFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 18:08 UTC
- Ora modificata: 5 dicembre 2017, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ComprehendMedicalFullAccess

Descrizione: Fornisce accesso completo ad Amazon Comprehend Medical

`ComprehendMedicalFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ComprehendMedicalFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 17:55 UTC
- Ora modificata: 27 novembre 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ComprehendReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon Comprehend.

`ComprehendReadOnly`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `ComprehendReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 18:10 UTC
- Ora modificata: 26 aprile 2022, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectDominantLanguage",
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:DetectEntities",
        "comprehend:BatchDetectEntities",
```

```
        "comprehend:DetectKeyPhrases",
        "comprehend:BatchDetectKeyPhrases",
        "comprehend:DetectPiiEntities",
        "comprehend:ContainsPiiEntities",
        "comprehend:DetectSentiment",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectSyntax",
        "comprehend:BatchDetectSyntax",
        "comprehend:ClassifyDocument",
        "comprehend:DescribeTopicsDetectionJob",
        "comprehend:ListTopicsDetectionJobs",
        "comprehend:DescribeDominantLanguageDetectionJob",
        "comprehend:ListDominantLanguageDetectionJobs",
        "comprehend:DescribeEntitiesDetectionJob",
        "comprehend:ListEntitiesDetectionJobs",
        "comprehend:DescribeKeyPhrasesDetectionJob",
        "comprehend:ListKeyPhrasesDetectionJobs",
        "comprehend:DescribePiiEntitiesDetectionJob",
        "comprehend:ListPiiEntitiesDetectionJobs",
        "comprehend:DescribeSentimentDetectionJob",
        "comprehend:DescribeTargetedSentimentDetectionJob",
        "comprehend:ListSentimentDetectionJobs",
        "comprehend:ListTargetedSentimentDetectionJobs",
        "comprehend:DescribeDocumentClassifier",
        "comprehend:ListDocumentClassifiers",
        "comprehend:DescribeDocumentClassificationJob",
        "comprehend:ListDocumentClassificationJobs",
        "comprehend:DescribeEntityRecognizer",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListTagsForResource",
        "comprehend:DescribeEndpoint",
        "comprehend:ListEndpoints",
        "comprehend:ListDocumentClassifierSummaries",
        "comprehend:ListEntityRecognizerSummaries",
        "comprehend:DescribeResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ComputeOptimizerAutomationServiceRolePolicy

Descrizione: la policy ComputeOptimizerAutomationServiceRolePolicy gestita è associata a un ruolo collegato al servizio che consente a Compute Optimizer di eseguire azioni per conto dell'utente

`ComputeOptimizerAutomationServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 novembre 2025, 01:19 UTC
- Ora modificata: 15 novembre 2025, 01:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerAutomationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSVolumeModification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/exclude-from-compute-optimizer-automation" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEBSSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RollbackEBSVolumeDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ComputeOptimizerReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a ComputeOptimizer.

`ComputeOptimizerReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ComputeOptimizerReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 7 marzo 2020, 00:11 UTC
- Ora modificata: 20 novembre 2024, 21:08 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "computeOptimizerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
```

```
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetIdleRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "cloudwatch:GetMetricData",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ComputeOptimizerServiceRolePolicy

Descrizione: consente di ComputeOptimizer chiamare AWS i servizi e raccogliere i dettagli del carico di lavoro per tuo conto.

`ComputeOptimizerServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 03 dicembre 2019, 08:45 UTC
- Ora modificata: 27 maggio 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ComputeOptimizerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingAccess",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElastiCacheAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServerlessCaches"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MemoryDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "memorydb:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DocumentDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesConnectionStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ConfigConformsServiceRolePolicy

Descrizione: policy necessaria per AWSConfig creare pacchetti di conformità

`ConfigConformsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 25 luglio 2019, 21:38 UTC
- Ora modificata: 12 gennaio 2023, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeRemediationConfigurations",
        "config:DeleteRemediationConfiguration",
        "config:PutRemediationConfigurations"
      ],
      "Resource" : "arn:aws:config:*:*:remediation-configuration/aws-service-
remediation-configuration/config-conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "remediation.config.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::awsconfigconforms*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetStackPolicy",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:ValidateTemplate",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awsconfigconforms-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Config"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ConsoleFullAccessFromVercel

Descrizione: Da utilizzare con account creati tramite l'integrazione di Vercel Marketplace con AWS. Fornisce l'accesso per gestire tutte le risorse per i servizi integrati con Vercel Marketplace.

`ConsoleFullAccessFromVercel`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ConsoleFullAccessFromVercel` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2025, 16:49 UTC
- Ora modificata: 09 aprile 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleFullAccessFromVercel`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dsql:UpdateCluster",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:ConditionCheckItem",
        "dynamodb:UntagResource",
        "dynamodb:PutItem",
        "dynamodb:ListTables",
        "dynamodb:DeleteItem",
        "dynamodb:Scan",
        "dynamodb:ListTagsOfResource",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:DescribeLimits",
        "dynamodb:UpdateTable",
        "dynamodb:GetRecords"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds-db:connect",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "rds:RebootDBInstance",
        "rds:DeleteDBInstance",
        "rds:StartDBInstance",
        "rds:ModifyDBInstance",
        "rds:ApplyPendingMaintenanceAction",
        "rds:StartDBCluster",
        "rds:DeleteDBCluster",
        "rds:RebootDBCluster",
```

```
        "rds:CreateDBClusterEndpoint",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:FailoverDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:ModifyDBClusterParameterGroup",
        "rds:CopyDBClusterParameterGroup",
        "rds:ResetDBClusterParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:ModifyDBParameterGroup",
        "rds:CopyDBParameterGroup",
        "rds:DeleteDBParameterGroup",
        "rds:CreateDBParameterGroup",
        "rds:DeleteDBClusterAutomatedBackup",
        "rds:CopyDBClusterSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:CreateDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AuroraRestricted",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "aurora-postgresql"
        }
      }
    },
    {
      "Sid" : "OpenSearchServerless",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll",
        "aoss:DashboardsAccessAll",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:CreateIndex",
        "aoss:DeleteIndex",
        "aoss:GetAccessPolicy",
        "aoss:GetIndex",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListSecurityPolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListTagsForResource",
        "aoss:TagResource",
        "aoss:UntagResource",
        "aoss:AddCollectionToCollectionGroup",
        "aoss:UpdateAccessPolicy",
        "aoss:UpdateCollection",
        "aoss:UpdateCollectionGroup",
        "aoss:UpdateIndex",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OpenSearchApplications",
      "Effect" : "Allow",
      "Action" : [
        "es:GetApplication",
        "es:UpdateApplication",
        "es:ListApplications",
        "es:GetDefaultApplicationSetting"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ViewFreeTierState",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ConsoleViewOnlyAccessFromVercel

Descrizione: Da utilizzare con account creati tramite l'integrazione di Vercel Marketplace con AWS. Fornisce l'accesso per visualizzare tutte le risorse per i servizi integrati con Vercel Marketplace.

`ConsoleViewOnlyAccessFromVercel`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ConsoleViewOnlyAccessFromVercel` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2025, 16:49 UTC
- Ora modificata: 09 aprile 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleViewOnlyAccessFromVercel`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
```

```
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OpenSearchServerless",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:GetAccessPolicy",
        "aoss:GetIndex",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListSecurityPolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OpenSearchApplications",
      "Effect" : "Allow",
      "Action" : [
        "es:GetApplication",
        "es:ListApplications"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewFreeTierState",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CostOptimizationHubAdminAccess

Descrizione: questa policy gestita fornisce l'accesso amministrativo al Cost Optimization Hub.

`CostOptimizationHubAdminAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CostOptimizationHubAdminAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 dicembre 2023, 00:03 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:UpdatePreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
```

```
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CostOptimizationHubReadOnlyAccess

Descrizione: questa policy gestita fornisce l'accesso in sola lettura al Cost Optimization Hub.

`CostOptimizationHubReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `CostOptimizationHubReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 dicembre 2023, 18:04 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CostOptimizationHubServiceRolePolicy

Descrizione: consente a Cost Optimization Hub di recuperare le informazioni sull'organizzazione e raccogliere dati e metadati relativi all'ottimizzazione.

`CostOptimizationHubServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 26 novembre 2023, 08:03 UTC
- Ora modificata: 17 luglio 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "CostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:GetCostAndUsage",
        "ce:GetDimensionValues"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

CustomerProfilesServiceLinkedRolePolicy

Descrizione: consente ai profili cliente di Amazon Connect di accedere a AWS servizi e risorse per tuo conto.

`CustomerProfilesServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 7 marzo 2023 22:56 UTC
- Ora modificata: 5 marzo 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/CustomerProfiles"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/
AWSServiceRoleForProfile_*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:PutProfileOutboundRequestBatch"
      ],
      "Resource" : [
        "arn:aws:connect-campaigns:*:*:campaign/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "profile:BatchGetProfile",
        "profile:GetRecommender",
        "profile:GetCalculatedAttributeForProfile",
        "profile:GetProfileRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DatabaseAdministrator

Descrizione: concede le autorizzazioni di accesso completo ai AWS servizi e alle azioni necessarie per impostare e configurare i servizi di AWS database.

`DatabaseAdministrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `DatabaseAdministrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:25 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:Describe*",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticache:*",
        "iam:ListRoles",
        "iam:GetRole",
        "kms:ListKeys",
        "lambda:CreateEventSourceMapping",
        "lambda:CreateFunction",
        "lambda:DeleteEventSourceMapping",
```

```
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:Create*",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "pi:CreatePerformanceAnalysisReport",
        "pi:DeletePerformanceAnalysisReport",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetPerformanceAnalysisReport",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pi:ListPerformanceAnalysisReports",
        "pi:ListTagsForResource",
        "pi:TagResource",
        "pi:UntagResource",
        "rds:*",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Get*",
        "sns:List*",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
```

```
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutLifecycleConfiguration",
        "s3:PutReplicationConfiguration",
        "s3:PutObject*",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/rdbms-lambda-access",
        "arn:aws:iam::*:role/lambda_exec_role",
        "arn:aws:iam::*:role/lambda-dynamodb-*",
        "arn:aws:iam::*:role/lambda-vpc-execution-role",
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DataScientist

Descrizione: concede le autorizzazioni ai servizi di analisi AWS dei dati.

`DataScientist`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `DataScientist` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:28 UTC
- Ora modificata: 03 dicembre 2019, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:*",
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "datapipeline:Describe*",
        "datapipeline:ListPipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:QueryObjects",
```

```
        "dynamodb:*",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotInstances",
        "ec2:RequestSpotFleet",
        "elasticfilesystem:*",
        "elasticmapreduce:*",
        "es:*",
        "firehose:*",
        "fsx:DescribeFileSystems",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "kinesis:*",
        "kms:List*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:PublishVersion",
        "lambda:Update*",
        "lambda:List*",
        "machinelearning:*",
        "sdb:*",
        "rds:*",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Abort*",
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketCors",
        "s3:PutBucketLogging",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
        "arn:aws:iam::*:role/EMR_DefaultRole",
        "arn:aws:iam::*:role/kinesis-*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:*App",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DAXServiceRolePolicy

Descrizione: questa politica consente a DAX di creare e gestire l'interfaccia di rete, il gruppo di sicurezza, la sottorete e il Vpc per conto del cliente

`DAXServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 5 marzo 2018, 17:51 UTC
- Ora modificata: 5 marzo 2018, 17:51 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DBModDiscoveryAndAssessment

Descrizione: autorizzazioni di individuazione e valutazione per il connettore di database utilizzato nella modernizzazione del database

`DBModDiscoveryAndAssessment`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `DBModDiscoveryAndAssessment` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 marzo 2026, 20:27 UTC
- Ora modificata: 25 marzo 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/DBModDiscoveryAndAssessment`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeInternetGateways",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "dms:DescribeEndpoints",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeOrderableReplicationInstances",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ModifyReplicationSubnetGroup",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:ModifyDBSubnetGroup",
      "Resource" : "arn:aws:rds:*:*:subgrp:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:EnableHttpEndpoint",
        "rds:DisableHttpEndpoint",
        "rds-data:ExecuteStatement"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeTableStatistics",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTaskIndividualAssessments",
        "dms:DescribeApplicableIndividualAssessments"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*",
        "arn:aws:dms:*:*:assessment-run:*",
        "arn:aws:dms:*:*:instance-profile:*",
        "arn:aws:dms:*:*:data-provider:*",
        "arn:aws:dms:*:*:migration-project:*",
        "arn:aws:dms:*:*:rep:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:ListMetadataModelAssessments",
        "dms:ListMetadataModelConversions",
        "dms:ListMetadataModelExports",
        "dms:DescribeMetadataModelImports",
        "dms:DescribeConversionConfiguration",
        "dms:DescribeMetadataModelCreations",
        "dms:DescribeMetadataModel",
        "dms:DescribeMetadataModelChildren",
        "dms:GetTargetSelectionRules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/dms-vpc-role",
        "arn:aws:iam::*:role/dms-cloudwatch-logs-role",
        "arn:aws:iam::*:role/dms-secrets-manager-role",
        "arn:aws:iam::*:role/dms-s3-access-role",
        "arn:aws:iam::*:role/aws-service-role/dms.amazonaws.com/
AWSServiceRoleForDMSServerless"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole",
        "arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:SecretArn" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DBModProvisioningAndMigration

Descrizione: autorizzazioni per la fornitura di risorse e la migrazione dei dati per il connettore di database utilizzato nella modernizzazione del database

`DBModProvisioningAndMigration`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `DBModProvisioningAndMigration` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 marzo 2026, 20:42 UTC
- Ora modificata: 25 marzo 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/DBModProvisioningAndMigration`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:UpdateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-db-modernization-*",
        "arn:aws:s3:::atx-db-modernization-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationSubnetGroup",
        "dms:CreateInstanceProfile",
        "dms:CreateDataProvider",
        "dms:CreateMigrationProject",
        "dms:CreateEndpoint",
        "dms:AddTagsToResource",
        "rds:CreateDBSubnetGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBInstance",
```

```
        "rds:AddTagsToResource",
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:subgrp:*",
        "arn:aws:dms:*:*:instance-profile:*",
        "arn:aws:dms:*:*:data-provider:*",
        "arn:aws:dms:*:*:migration-project:*",
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db:*",
        "arn:aws:ec2:*:*:vpc-endpoint:*",
        "arn:aws:dms:*:*:endpoint:*",
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:ExportMetadataModelAssessment",
        "dms:StartMetadataModelImport",
        "dms:StartMetadataModelConversion",
        "dms:StartMetadataModelExportToTarget",
        "dms:StartMetadataModelExportAsScripts",
        "dms:StartMetadataModelAssessment",
        "dms:StartMetadataModelCreation",
        "dms:UpdateConversionConfiguration",
        "dms:UpdateMigrationProject",
        "dms:AddTagsToResource",
        "dms:ListTagsForResource",
        "dms:DeleteMigrationProject",
        "dms:DeleteEndpoint",
        "dms:UpdateInstanceProfile",
        "dms:UpdateDataProvider",
        "dms:DeleteInstanceProfile",
```

```
        "dms:DeleteDataProvider",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:migration-project:*",
        "arn:aws:dms:*:*:instance-profile:*",
        "arn:aws:dms:*:*:data-provider:*",
        "arn:aws:dms:*:*:endpoint:*",
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:DeleteReplicationInstance",
        "dms:ModifyReplicationInstance",
        "dms:RebootReplicationInstance"
      ],
      "Resource" : "arn:aws:dms:*:*:rep:*",
      "Condition" : {
        "StringEquals" : {
          "dms:rep-tag/Project" : "atx-db-modernization",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:DeleteReplicationTask",
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:StartReplicationTaskAssessmentRun",
        "dms:CancelReplicationTaskAssessmentRun"
      ],
```

```
      "Resource" : [
        "arn:aws:dms:*:*:task:*",
        "arn:aws:dms:*:*:assessment-run:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "dms:task-tag/Project" : "atx-db-modernization",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/dms-vpc-role",
        "arn:aws:iam::*:role/dms-cloudwatch-logs-role",
        "arn:aws:iam::*:role/dms-secrets-manager-role",
        "arn:aws:iam::*:role/dms-s3-access-role",
        "arn:aws:iam::*:role/DMSPremigrationAssessmentS3Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "iam:PassedToService" : [
            "dms.amazonaws.com",
            "dms.*.amazonaws.com",
            "schema-conversion.dms.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        },
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DBModVirtualSource

Descrizione: fornisce le autorizzazioni per il connettore di database utilizzato da ATxHelix durante il flusso di lavoro di modernizzazione del database offline () DMS-free

`DBModVirtualSource`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `DBModVirtualSource` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 luglio 2026, 23:12 UTC
- Ora modificata: 6 luglio 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/DBModVirtualSource`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInternetGateways",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:ModifyDBSubnetGroup",
      "Resource" : "arn:aws:rds:*:*:subgrp:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:EnableHttpEndpoint",
        "rds:DisableHttpEndpoint",
```

```
        "rds-data:ExecuteStatement"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:SecretArn" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:UpdateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-db-modernization-*",
        "arn:aws:s3:::atx-db-modernization-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSubnetGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBInstance",
        "rds:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DeclarativePoliciesEC2Report

Descrizione: fornisce l'accesso alle API di sola lettura necessarie per eseguire l'EC2 Declarative Policies Account Status Report.

`DeclarativePoliciesEC2Report`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 30 novembre 2024, 13:21 UTC
- Ora modificata: 03 luglio 2026, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DeclarativePoliciesEC2Report`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeclarativePoliciesEC2Report",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetAllowedImagesSettings",
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeAccountVpcEncryptionControl"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

Descrizione: autorizzazioni necessarie per supportare Amazon CloudWatch Contributor Insights per Amazon DynamoDB.

`DynamoDBCloudWatchContributorInsightsServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 novembre 2019, 21:13 UTC
- Ora modificata: 15 novembre 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteInsightRules",
        "cloudwatch:PutInsightRule"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "cloudwatch:DescribeInsightRules"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DynamoDBGlobalTableSettingsManagementServiceRolePolicy

Descrizione: Autorizzazioni richieste da DynamoDB per gestire le impostazioni globali di replica delle tabelle

`DynamoDBGlobalTableSettingsManagementServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 ottobre 2025, 17:34 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBGlobalTableSettingsManagementServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededToReplicateSettings",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*",
        "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/dynamodb/table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : [
            "dynamodb"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DynamoDBKinesisReplicationServiceRolePolicy

Descrizione: Fornire l'accesso a AWS DynamoDB a KinesisDataStreams

`DynamoDBKinesisReplicationServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 novembre 2020, 00:43 UTC
- Ora modificata: 12 novembre 2020, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "kinesis.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

DynamoDBReplicationServiceRolePolicy

Descrizione: Autorizzazioni richieste da DynamoDB per la replica dei dati tra regioni

`DynamoDBReplicationServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 9 novembre 2017, 23:55 UTC
- Ora modificata: 08 gennaio 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "dynamodb:Scan",
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
```

```
        "dynamodb:DescribeTimeToLive",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:DescribeLimits",
        "dynamodb:GetResourcePolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

EC2ApplicationStatusChecksServiceRolePolicy

Descrizione: consente a EC2 di scoprire e gestire le risorse relative ai controlli dello stato delle applicazioni EC2

`EC2ApplicationStatusChecksServiceRolePolicy`è una policy AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 27 aprile 2026, 23:42 UTC
- Ora modificata: 15 luglio 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2ApplicationStatusChecksServiceRolePolicy`

Versione della politica

Versione della politica: v3 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : [
            "ec2.application-status-checks.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Usage"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

EC2FastLaunchFullAccess

Descrizione: questa politica garantisce l'accesso completo alle azioni di EC2 Fast Launch

`EC2FastLaunchFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `EC2FastLaunchFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 maggio 2024, 22:45 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/EC2FastLaunchFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2FastLaunch",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch",
        "ec2:DisableFastLaunch",
        "ec2:DescribeFastLaunchImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CreateVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ModifyDeleteVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:CreateSubnet",
        "ec2:ModifyVpcAttribute",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
```

```
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSecurityGroup",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ManageSecurityGroupEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:RollbackStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/EC2FastLaunch*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchTemplateModify",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyLaunchTemplate",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
```

```
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "EC2LaunchInstanceWithVolAndInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "EC2Tags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
```

```
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "EC2ManageTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2fastlaunch.amazonaws.com/
AWSServiceRoleForEC2FastLaunch",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLRPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
```

```
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

EC2FastLaunchServiceRolePolicy

Descrizione: la politica consente a ec2fastlaunch di preparare e gestire istantanee preimpostate nell'account del cliente e pubblicare le relative metriche.

`EC2FastLaunchServiceRolePolicy`è una AWS politica gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 gennaio 2022, 13:08 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRunInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "AllowRunInstancesOnFastLaunchCreatedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStopAndTerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTaggedSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "StringLike" : {
          "aws:RequestTag/CreatedByLaunchTemplateVersion" : "*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedByLaunchTemplateName",
            "CreatedByLaunchTemplateId"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDeleteSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDeleteVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
```

```
    {
      "Sid" : "AllowDeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeVolumes",
        "ec2:DescribeNetworkInterfaces",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EC2"
        }
      }
```

```
    },
    {
      "Sid" : "AllowEventsRuleMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2fastlaunch.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowEventsRuleNonMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowKMSActions",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeleteFastLaunchLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

EC2FleetTimeShiftableServiceRolePolicy

Descrizione: politica che concede le autorizzazioni a EC2 Fleet per lanciare istanze in futuro.

`EC2FleetTimeShiftableServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 23 dicembre 2019, 19:47 UTC
- Ora modificata: 23 dicembre 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

Ec2ImageBuilderCrossAccountDistributionAccess

Descrizione: le autorizzazioni necessarie a EC2 Image Builder per eseguire una distribuzione tra account.

`Ec2ImageBuilderCrossAccountDistributionAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `Ec2ImageBuilderCrossAccountDistributionAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 30 settembre 2020, 19:22 UTC
- Ora modificata: 30 settembre 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::image/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

EC2ImageBuilderExecutionPolicy

Descrizione: concede le autorizzazioni che consentono a EC2 Image Builder di chiamare i servizi per tuo conto AWS

`EC2ImageBuilderExecutionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `EC2ImageBuilderExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 giugno 2026, 17:12 UTC
- Ora modificata: 08 luglio 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/EC2ImageBuilderExecutionPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "RunInstancesWithEC2ImageBuilderRequestTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
```

```
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2InstanceStateChangePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CopyImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CreateImagePermissionsForImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2CreateImagePermissionsForInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeregisterImagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2RegisterImagePermissionsForImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2RegisterImagePermissionsForSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2ModifyImageAttributePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2SnapshotAttributeModificationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ],
          "ec2:CreateAction" : [
            "CreateImage",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCustomerTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Sid" : "CreateEC2ImageBuilderTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Sid" : "AttachImageWatermarkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachImageWatermark"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "UpdateCustomerLicensePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : [
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "PublishNotificationToCustomerSNSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SystemsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListInventoryEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SystemsManagerPermissionsForAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
```

```
      "Sid" : "SystemsManagerPermissionsForInstance",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceAssociationsStatus"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SendCommandDocumentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep"
      ]
    },
    {
      "Sid" : "SendCommandEC2ImageBuilderInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "InventoryCollectionAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
```

```
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory"
      ]
    },
    {
      "Sid" : "InventoryCollectionInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "InventoryCollectionTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "DeleteInventoryCollectionAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
```

```
      "Sid" : "EC2KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2KMSDescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2KMSGrantKeyPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountAssumeRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
      ]
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
      ]
    },
    {
      "Sid" : "LaunchTemplatePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExportImageBuilderImagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "CreateExportImageTaskPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Sid" : "CancelExportImageTaskPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:export-image-task/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
```

```
        }
      }
    },
    {
      "Sid" : "CreateSLRForOtherServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EnableFastLaunchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "ListInspectorFindingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CreateECRImageForInspectorScanningPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/image-builder-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "DeleteECRImageForInspectorScanningPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/image-builder-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EventBridgePermissionsForInspectorScanning",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
```

```
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    },
    {
      "Sid" : "ParameterStorePermissionsForImageBuilderParameters",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/imagebuilder/*"
      ]
    },
    {
      "Sid" : "ParameterStorePermissionsForServiceManagedParameters",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*::parameter/aws/service/*"
      ]
    },
    {
      "Sid" : "StartImagePipelineExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:StartImagePipelineExecution",
        "imagebuilder:TagResource"
      ],
      "Resource" : [
        "arn:aws:imagebuilder:*:*:image-pipeline/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

EC2ImageBuilderLifecycleExecutionPolicy

Descrizione: la EC2 ImageBuilderLifecycleExecutionPolicy politica concede a Image Builder le autorizzazioni per eseguire azioni come deprecare o eliminare le risorse di immagine di Image Builder e le relative AMIs risorse sottostanti (istantanee) per supportare regole automatizzate per le attività di gestione del ciclo di vita delle immagini.

`EC2ImageBuilderLifecycleExecutionPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `EC2ImageBuilderLifecycleExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 16 novembre 2023, 23:23 UTC
- Ora modificata: 16 novembre 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
```

```
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "DeprecatedBy"
        }
      }
    },
    {
      "Sid" : "ECRImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "ImageBuilderEC2TagServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "tag:GetResources",
        "imagebuilder:DeleteImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

EC2InstanceConnect

Descrizione: consente ai clienti di chiamare EC2 Instance Connect per pubblicare chiavi temporanee sulle proprie istanze EC2 e connettersi tramite ssh o l'EC2 Instance Connect CLI.

`EC2InstanceConnect`è una policy gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `EC2InstanceConnect` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 giugno 2019, 18:53 UTC
- Ora modificata: 27 giugno 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
```

```
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

Ec2InstanceConnectEndpoint

Descrizione: policy degli endpoint EC2 Instance Connect per gestire gli endpoint EC2 Instance Connect creati dal cliente

`Ec2InstanceConnectEndpoint`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 24 gennaio 2023, 20:19 UTC
- Ora modificata: 31 luglio 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:ModifyNetworkInterfaceAttribute",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

EC2InstanceProfileForImageBuilder

Descrizione: profilo di istanza EC2 per il servizio Image Builder.

`EC2InstanceProfileForImageBuilder`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `EC2InstanceProfileForImageBuilder` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 01 dicembre 2019, 19:08 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot",
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*.ISO",
        "arn:aws:s3:::*/*.iso",
        "arn:aws:s3:::*/*.Iso"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetMarketplaceResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

EC2InstanceProfileForImageBuilderECRContainerBuilds

Descrizione: profilo di istanza EC2 per la creazione di immagini di container con EC2 Image Builder. Questa politica concede all'utente ampie autorizzazioni per caricare immagini ECR.

`EC2InstanceProfileForImageBuilderECRContainerBuilds`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `EC2InstanceProfileForImageBuilderECRContainerBuilds` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 dicembre 2020, 19:48 UTC
- Ora modificata: 11 dicembre 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ECRReplicationServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da ECR Replication

`ECRReplicationServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 4 dicembre 2020, 22:11 UTC
- Ora modificata: 04 dicembre 2020, 22:11 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ECRTemplateServiceRolePolicy

Descrizione: consente di eseguire azioni quando si utilizzano modelli di creazione di repository AWS ECR

`ECRTemplateServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 19 giugno 2024, 23:11 UTC
- Ora modificata: 19 giugno 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRTemplateServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateRepositoryWithTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ElastiCacheServiceRolePolicy

Descrizione: questa politica consente di ElastiCache gestire AWS le risorse per conto dell'utente nella misura necessaria alla gestione della cache

`ElastiCacheServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 7 dicembre 2017, 17:50 UTC
- Ora modificata: 28 novembre 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ElasticLoadBalancingFullAccess

Descrizione: fornisce accesso completo ad Amazon ElasticLoadBalancing e accesso limitato ad altri servizi necessari per fornire ElasticLoadBalancing funzionalità.

`ElasticLoadBalancingFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ElasticLoadBalancingFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 settembre 2018, 20:42 UTC
- Ora modificata: 23 febbraio 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
```

```
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "cognito-idp:DescribeUserPoolClient"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:*",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ElasticLoadBalancingReadOnly

Descrizione: Fornisce accesso in sola lettura ad Amazon ElasticLoadBalancing e ai servizi dipendenti

`ElasticLoadBalancingReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ElasticLoadBalancingReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 settembre 2018, 20:17 UTC
- Ora modificata: 26 novembre 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement3",
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:GetManagedResource",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Sid" : "Statement4",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ElementalActivationsDownloadSoftwareAccess

Descrizione: Accesso per visualizzare gli asset acquistati e scaricare il software correlato e i file kickstart

`ElementalActivationsDownloadSoftwareAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ElementalActivationsDownloadSoftwareAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 8 settembre 2020, 17:26 UTC
- Ora modificata: 08 settembre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ElementalActivationsFullAccess

Descrizione: accesso completo alla visualizzazione e all'adozione di misure relative alle apparecchiature elementari e ai software acquistati

`ElementalActivationsFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ElementalActivationsFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 4 giugno 2020, 21:00 UTC
- Ora modificata: 4 giugno 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ElementalActivationsGenerateLicenses

Descrizione: accesso per visualizzare gli asset acquistati e generare licenze software per le attivazioni in sospeso

`ElementalActivationsGenerateLicenses`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `ElementalActivationsGenerateLicenses` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 agosto 2020, 18:28 UTC
- Ora modificata: 28 agosto 2020, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ElementalActivationsReadOnlyAccess

Descrizione: accesso in sola lettura all'elenco dettagliato degli asset acquistati associati all' Account AWS utente

`ElementalActivationsReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ElementalActivationsReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 agosto 2020, 16:51 UTC
- Ora modificata: 28 agosto 2020, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ElementalAppliancesSoftwareFullAccess

Descrizione: accesso completo per visualizzare e intervenire sui preventivi e sugli ordini di elettrodomestici e software elementali

`ElementalAppliancesSoftwareFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ElementalAppliancesSoftwareFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 31 luglio 2019, 16:28 UTC
- Ora modificata: 5 febbraio 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ElementalAppliancesSoftwareReadOnlyAccess

Descrizione: accesso in sola lettura per visualizzare i preventivi e gli ordini di elettrodomestici e software elementali

`ElementalAppliancesSoftwareReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `ElementalAppliancesSoftwareReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 1 aprile 2020, 22:31 UTC
- Ora modificata: 01 aprile 2020, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ElementalSupportCenterFullAccess

Descrizione: accesso completo per visualizzare e intervenire sui casi di supporto relativi a dispositivi e software Elemental Appliance e ai contenuti di supporto ai prodotti

`ElementalSupportCenterFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ElementalSupportCenterFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 novembre 2020, 18:08 UTC
- Ora modificata: 5 febbraio 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

EMRDescribeClusterPolicyForEMRWAL

Descrizione: questa politica concede autorizzazioni di sola lettura che consentono al servizio WAL per Amazon EMR di trovare e restituire lo stato di un cluster

`EMRDescribeClusterPolicyForEMRWAL`AWS è una politica gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 giugno 2023, 23:30 UTC
- Ora modificata: 15 giugno 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

FinOpsAgentAgentPolicy

Descrizione: fornisce le autorizzazioni richieste dall' AWS FinOps agente per eseguire l'analisi dei costi e individuare opportunità di risparmio sui costi sulle AWS risorse dei clienti.

`FinOpsAgentAgentPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `FinOpsAgentAgentPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 giugno 2026, 19:57 UTC
- Ora modificata: 03 giugno 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/FinOpsAgentAgentPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FinOpsAgentDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostForecast",
        "ce:GetUsageForecast",
        "ce:GetDimensionValues",
        "ce:GetTags",
        "ce:GetCostCategories",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostComparisonDrivers",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetReservationCoverage",
        "ce:GetReservationUtilization",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:DescribeCostCategoryDefinition",
        "ce:ListCostCategoryDefinitions",
        "budgets:ViewBudget",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
```

```
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetIdleRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "freetier:GetFreeTierUsage",
        "bcm-pricing-calculator:GetPreferences",
        "bcm-pricing-calculator:GetWorkloadEstimate",
        "bcm-pricing-calculator:ListWorkloadEstimateUsage",
        "bcm-pricing-calculator:ListWorkloadEstimates",
        "cloudtrail:LookupEvents",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
```

```
        "cloudwatch:ListMetrics",
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeManagedRuleManagementWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:EnableRule",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "finops-agent.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeManagedRuleManagementReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

FinOpsAgentOperatorPolicy

Descrizione: fornisce l'accesso all'utilizzo dell'app Web AWS FinOps Agent per un agente.

`FinOpsAgentOperatorPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `FinOpsAgentOperatorPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 giugno 2026, 19:57 UTC
- Ora modificata: 03 giugno 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/FinOpsAgentOperatorPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "FinOpsAgentOperatorAccess",
      "Effect" : "Allow",
      "Action" : [
        "finops-agent:CreateConversation",
        "finops-agent:ListConversations",
        "finops-agent:CreateTurn",
        "finops-agent:GetTurn",
        "finops-agent:ListTurns",
        "finops-agent:CancelTurn",
        "finops-agent:AcceptAgentRequest",
        "finops-agent:RejectAgentRequest",
        "finops-agent:GetAgentRequest",
        "finops-agent:CreateTask",
        "finops-agent:GetTask",
        "finops-agent:ListTasks",
        "finops-agent:CancelTask",
        "finops-agent:CreateAutomation",
        "finops-agent:GetAutomation",
        "finops-agent:ListAutomations",
        "finops-agent:UpdateAutomation",
        "finops-agent:DeleteAutomation",
        "finops-agent:CreateDocument",
        "finops-agent:GetDocumentContent",
        "finops-agent:GetDocumentMetadata",
        "finops-agent:ListDocuments",
        "finops-agent:UpdateDocument",
        "finops-agent:DeleteDocument",
        "finops-agent:RestoreDocument",
        "finops-agent:GetArtifactContent",
        "finops-agent:GetArtifactMetadata",
        "finops-agent:DeleteArtifact",
        "finops-agent:ListArtifacts",
        "finops-agent:ListRecords",
        "finops-agent:SendFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

FMSServiceRolePolicy

Descrizione: politica di accesso per consentire al ruolo collegato al servizio FM di eseguire azioni relative a FM sulle risorse gestite da FM all'interno dell'account dell'organizzazione del cliente. AWS

`FMSServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 28 marzo 2018, 23:01 UTC
- Ora modificata: 6 aprile 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Versione della politica

Versione della politica: v37 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WafGeneral",
```

```
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
      ]
    },
```

```
    {
      "Sid" : "WafWebaclCreation",
      "Effect" : "Allow",
      "Action" : [
        "waf:CreateWebACL",
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
      ]
    },
    {
      "Sid" : "ElbGeneral",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WafPermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf:DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",
        "waf-regional:GetPermissionPolicy",
        "waf-regional:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
      ]
    },
    {
      "Sid" : "CloudfrontGeneral",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudfrontVpcOriginAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetVpcOrigin"
      ],
      "Resource" : "arn:aws:cloudfront::*:vpcorigin/*"
    },
    {
      "Sid" : "ConfigScoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation",
        "config:DeleteEvaluationResults"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
    },
    {
      "Sid" : "ConfigUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
```

```
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig",
        "config:BatchGetResourceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
      ]
    },
    {
      "Sid" : "OrganizationsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ShieldGeneral",
      "Effect" : "Allow",
      "Action" : [
```

```
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:ListAttacks",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:UpdateEmergencyContactSettings",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeAddresses",
        "shield:EnableApplicationLayerAutomaticResponse",
        "shield:DisableApplicationLayerAutomaticResponse",
        "shield:UpdateApplicationLayerAutomaticResponse"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2SecurityGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SecurityGroupTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "SecurityGroupTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/FMManaged" : "*"
        }
      }
    },
    {
      "Sid" : "Ec2Unscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:AssociateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Wafv2General",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "Wafv2WebAclAndRuleGroupMutation",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
```

```
      ]
    },
    {
      "Sid" : "Wafv2PermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Sid" : "Wafv2WebaclDescribe",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "RouteTableTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SubnetTagManagement",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RouteTableCleanup",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "Ec2DescribeUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateVpcEndpointScoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "CreateVpcEndpointUnscoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VpcEndpointsDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:resource-share/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RamMutation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamCreation",
      "Effect" : "Allow",
      "Action" : "ram:CreateResourceShare",
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "RamDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "network-firewall.amazonaws.com",
            "shield.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamDescribe",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "NetworkFirewallTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "NetworkFirewallGeneral",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListTLSInspectionConfigurations"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "NetworkFirewallResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:firewall-policy/*",
        "arn:aws:network-firewall:*:*:stateful-rulegroup/*",
        "arn:aws:network-firewall:*:*:stateless-rulegroup/*"
      ]
    },
    {
      "Sid" : "NetworkFirewallCleanup",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LogsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
        "route53resolver:ListFirewallRuleGroups",
```

```
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupCleanup",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ResolverRuleGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl"
        }
      }
    },
    {
      "Sid" : "NaclTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkAclEntry",
        "ec2:CreateNetworkAclEntry",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateNetworkAcl"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

FSxDeleteServiceLinkedRoleAccess

Descrizione: consente FSx ad Amazon di eliminare i ruoli collegati ai servizi per l'accesso ad Amazon S3

`FSxDeleteServiceLinkedRoleAccess`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 28 novembre 2018, 10:40 UTC
- Ora modificata: 28 novembre 2018, 10:40 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

GameLiftContainerFleetPolicy

Descrizione: concede le autorizzazioni necessarie per le azioni di calcolo in una flotta di GameLift container Amazon, incluso l'accesso a dipendenze come Amazon S3.

`GameLiftContainerFleetPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `GameLiftContainerFleetPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 12 novembre 2024, 19:28 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftContainerFleetPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WriteGameSessionLogsToLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*:log-stream:*"
    },
    {
      "Sid" : "CreateLogGroupToStoreGameSessionLogs",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*"
    },
    {
      "Sid" : "WriteGameSessionLogsToS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::gamelift-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RetrieveComputeAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "gamelift:GetComputeAuthToken"
      ],
      "Resource" : [
        "arn:aws:gamelift:*:*:containerfleet/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

GameLiftGameServerGroupPolicy

Descrizione: Politica per consentire a Gamelift di GameServerGroups gestire le risorse dei clienti

`GameLiftGameServerGroupPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `GameLiftGameServerGroupPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 03 aprile 2020, 23:12 UTC
- Ora modificata: 13 maggio 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
```

```
        "autoscaling:ResumeProcesses",
        "autoscaling:EnterStandby",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:DetachInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sns:Publish",
      "Resource" : [
        "arn:*:sns:*:*:ActivatingLifecycleHookTopic-*",
        "arn:*:sns:*:*:TerminatingLifecycleHookTopic-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/GameLift"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

GitLabDuoWithAmazonQPermissionsPolicy

Descrizione: questa policy gestita concede l'autorizzazione a connettersi con Amazon Q e utilizzare le funzionalità dell'integrazione GitLab Duo con Amazon Q.

`GitLabDuoWithAmazonQPermissionsPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `GitLabDuoWithAmazonQPermissionsPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 aprile 2025, 16:37 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/GitLabDuoWithAmazonQPermissionsPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GitLabDuoUsagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:SendEvent",
        "q:CreateAuthGrant",
        "q:UpdateAuthGrant",
        "q:GenerateCodeRecommendations",
        "q:SendMessage",
        "q:ListPlugins",
        "q:VerifyOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateOAuthAppConnection",
        "q:DeleteOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoPluginPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin"
      ],
      "Resource" : "arn:aws:qdeveloper:*:*:plugin/GitLabDuoWithAmazonQ/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

GlobalAcceleratorFullAccess

Descrizione: consenti GlobalAccelerator agli utenti l'accesso completo a tutti APIs

`GlobalAcceleratorFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `GlobalAcceleratorFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 02:44 UTC
- Ora modificata: 04 dicembre 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "globalaccelerator:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "globalaccelerator.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

GlobalAcceleratorReadOnlyAccess

Descrizione: consenti GlobalAccelerator agli utenti l'accesso alla sola lettura APIs

`GlobalAcceleratorReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `GlobalAcceleratorReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 02:41 UTC
- Ora modificata: 27 novembre 2018, 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

GreengrassOTAUpdateArtifactAccess

Descrizione: Fornisce l'accesso in lettura agli artefatti Greengrass OTA Update in tutte le regioni Greengrass

`GreengrassOTAUpdateArtifactAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `GreengrassOTAUpdateArtifactAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 29 novembre 2017, 18:11 UTC
- Ora modificata: 18 dicembre 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

GroundTruthSyntheticConsoleFullAccess

Descrizione: questa politica concede le autorizzazioni necessarie per utilizzare tutte le funzionalità della console sintetica SageMaker Ground Truth.

`GroundTruthSyntheticConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `GroundTruthSyntheticConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 agosto 2022, 15:58 UTC

- Ora modificata: 25 agosto 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

GroundTruthSyntheticConsoleReadOnlyAccess

Descrizione: Questa politica garantisce l'accesso in sola lettura a SageMaker Ground Truth Synthetic tramite. Console di gestione AWS

`GroundTruthSyntheticConsoleReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `GroundTruthSyntheticConsoleReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 25 agosto 2022, 15:58 UTC
- Ora modificata: 25 agosto 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

Health_OrganizationsServiceRolePolicy

Descrizione: policy AWS Health per abilitare la funzionalità Organizational View

`Health_OrganizationsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 16 dicembre 2019, 13:28 UTC
- Ora modificata: 6 febbraio 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IAMAccessAdvisorReadOnly

Descrizione: questa policy consente l'accesso alla lettura di tutte le informazioni di accesso fornite da IAM Access Advisor, come le informazioni sull'ultimo accesso al servizio.

`IAMAccessAdvisorReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `IAMAccessAdvisorReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 21 giugno 2019, 19:33 UTC
- Ora modificata: 21 giugno 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GenerateOrganizationsAccessReport",
        "iam:GenerateCredentialReport",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetailsWithEntities",
        "iam:GetOrganizationsAccessReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IAMAccessAnalyzerFullAccess

Descrizione: fornisce l'accesso completo a IAM Access Analyzer

`IAMAccessAnalyzerFullAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `IAMAccessAnalyzerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 dicembre 2019, 17:12 UTC
- Ora modificata: 02 dicembre 2019, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IAMAccessAnalyzerReadOnlyAccess

Descrizione: fornisce accesso in sola lettura alle risorse di IAM Access Analyzer

`IAMAccessAnalyzerReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `IAMAccessAnalyzerReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 2 dicembre 2019, 17:12 UTC
- Ora modificata: 18 luglio 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckAccessNotGranted",
```

```
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:Get*",
        "access-analyzer:List*",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IAMFullAccess

Descrizione: fornisce l'accesso completo a IAM tramite Console di gestione AWS.

`IAMFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `IAMFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 21 giugno 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:*",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IAMReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a IAM tramite Console di gestione AWS.

`IAMReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `IAMReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:40 UTC
- Ora modificata: 25 gennaio 2018, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IAMSelfManageServiceSpecificCredentials

Descrizione: consente a un utente IAM di gestire le proprie credenziali specifiche del servizio.

`IAMSelfManageServiceSpecificCredentials`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `IAMSelfManageServiceSpecificCredentials` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 dicembre 2016, 17:25 UTC
- Ora modificata: 22 dicembre 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:ListServiceSpecificCredentials",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IAMUserChangePassword

Descrizione: offre la possibilità a un utente IAM di modificare la propria password.

`IAMUserChangePassword`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `IAMUserChangePassword` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 15 novembre 2016, 00:25 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC

- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}",
        "arn:aws:iam::*:user/*/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IAMUserSSHKeys

Descrizione: offre la possibilità a un utente IAM di gestire le proprie chiavi SSH.

`IAMUserSSHKeys`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `IAMUserSSHKeys` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 9 luglio 2015, 17:08 UTC
- Ora modificata: 9 luglio 2015, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
```

```
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IVSFullAccess

Descrizione: fornisce l'accesso completo a Interactive Video Service (IVS), include anche le autorizzazioni per i servizi dipendenti, necessarie per l'accesso completo alla console ivs.

`IVSFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `IVSFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 13 dicembre 2023, 21:20 UTC
- Ora modificata: 13 dicembre 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IVSReadOnlyAccess

Descrizione: fornisce accesso in sola lettura allo streaming IVS a bassa latenza e in tempo reale APIs

`IVSReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `IVSReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 5 dicembre 2023, 18:00 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
```

```
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantReplicas",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

IVSRecordToS3

Descrizione: Service Linked Role per eseguire da S3 PutObject alla registrazione di live streaming IVS

`IVSRecordToS3`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 5 dicembre 2020, 00:10 UTC
- Ora modificata: 05 dicembre 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

KafkaConnectServiceRolePolicy

Descrizione: questa politica concede a Kafka Connect l'autorizzazione a AWS gestire le risorse per tuo conto.

`KafkaConnectServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 07 settembre 2021, 13:12 UTC
- Ora modificata: 07 settembre 2021, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonMSKConnectManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonMSKConnectManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMSKConnectManaged" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

KafkaServiceRolePolicy

Descrizione: politica dei ruoli collegati al servizio IAM per Kafka.

`KafkaServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 novembre 2018, 23:31 UTC
- Ora modificata: 10 novembre 2025, 23:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeVpcEndpoints",
        "acm-pca:GetCertificateAuthorityCertificate",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
```

```
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "secretsmanager:SecretId" : "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:*:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

KeyspacesCDCServiceRolePolicy

Descrizione: concede le autorizzazioni necessarie ad Amazon Keyspaces for Change Data Capture

`KeyspacesCDCServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 21 giugno 2025, 00:22 UTC
- Ora modificata: 21 giugno 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesCDCServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Cassandra"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

KeyspacesReplicationServiceRolePolicy

Descrizione: autorizzazioni richieste da Keyspaces per la replica dei dati tra regioni

`KeyspacesReplicationServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 2 maggio 2023, 16:15 UTC
- Ora modificata: 15 novembre 2024, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:Modify",
        "cassandra:Alter",
        "cassandra:ModifyMultiRegionResource",
        "cassandra:SelectMultiRegionResource",
        "cassandra:AlterMultiRegionResource",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWDeleteAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*"
    },
    {
      "Sid" : "CWDescribeAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
```

```
    {
      "Sid" : "CWPutMetricAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "cloudwatch:AlarmActions" : [
            "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/cassandra/keyspace/*/
table/*:policyName/*:createdBy/*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

LakeFormationDataAccessServiceRolePolicy

Descrizione: Politica per concedere l'accesso temporaneo ai dati alle risorse di Lake Formation

`LakeFormationDataAccessServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 20 giugno 2019, 20:46 UTC
- Ora modificata: 6 febbraio 2024, 18:37 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

LexBotPolicy

Descrizione: Policy per il caso d'uso di AWS Lex Bot

`LexBotPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 febbraio 2017, 22:18 UTC
- Ora modificata: 13 novembre 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
```

```
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

LexChannelPolicy

Descrizione: Policy per il caso d'uso di AWS Lex Channel

`LexChannelPolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 febbraio 2017, 23:23 UTC
- Ora modificata: 17 febbraio 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

LightsailExportAccess

Descrizione: AWS politica dei ruoli collegati al servizio Lightsail che concede le autorizzazioni per esportare risorse

`LightsailExportAccess`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 28 settembre 2018, 16:35 UTC
- Ora modificata: 15 gennaio 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:DescribeSnapshots",
        "ec2:CopyImage",
        "ec2:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

MediaConnectGatewayInstanceRolePolicy

Descrizione: questa politica concede l'autorizzazione a registrare le istanze MediaConnect Gateway su un MediaConnect Gateway.

`MediaConnectGatewayInstanceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `MediaConnectGatewayInstanceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 22 marzo 2023, 20:43 UTC
- Ora modificata: 22 marzo 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

MediaPackageServiceRolePolicy

Descrizione: consente MediaPackage di pubblicare registri su CloudWatch

`MediaPackageServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 settembre 2020, 17:45 UTC
- Ora modificata: 18 settembre 2020, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

MemoryDBServiceRolePolicy

Descrizione: questa politica consente a MemoryDB di gestire AWS le risorse per conto dell'utente nella misura necessaria per la gestione delle risorse.

`MemoryDBServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 17 agosto 2021, 22:34 UTC
- Ora modificata: 01 dicembre 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateMemoryDBTagsOnNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "AmazonMemoryDBManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DeleteMemoryDBTaggedNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "DescribeEC2Resources",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutCloudWatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MemoryDB"
        }
      }
    },
    {
      "Sid" : "ReplicateMemoryDBMultiRegionClusterData",
      "Effect" : "Allow",
      "Action" : [
        "memorydb:ReplicateMultiRegionClusterData"
      ],
      "Resource" : "arn:aws:memorydb:*:*:cluster/*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

MigrationHubDMSAccessServiceRolePolicy

Descrizione: Politica per l'assunzione del ruolo del Database Migration Service nell'account del cliente per chiamare Migration Hub

`MigrationHubDMSAccessServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 giugno 2019, 17:50 UTC
- Ora modificata: 07 ottobre 2019, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
```

```
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

MigrationHubServiceRolePolicy

Descrizione: consente a Migration Hub di chiamare Application Discovery Service per conto dell'utente

`MigrationHubServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 giugno 2019, 17:22 UTC
- Ora modificata: 06 agosto 2020, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

MigrationHubSMSAccessServiceRolePolicy

Descrizione: Politica per l'assunzione del ruolo del servizio di migrazione dei server nell'account del cliente per chiamare Migration Hub

`MigrationHubSMSAccessServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 giugno 2019, 18:30 UTC
- Ora modificata: 07 ottobre 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
```

```
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

MonitronServiceRolePolicy

Descrizione: Policy per il ruolo collegato al servizio AWS Monitron che garantisce l'accesso alle risorse richieste del cliente.

`MonitronServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 2 maggio 2022, 19:22 UTC
- Ora modificata: 02 maggio 2022, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

MultiPartyApprovalFullAccess

Descrizione: fornisce l'accesso completo all'approvazione multipartitica. Questa policy include anche le autorizzazioni correlate a AWS Organizations e AWS IAM Identity per la gestione dei team di approvazione e delle fonti di identità.

`MultiPartyApprovalFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `MultiPartyApprovalFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 giugno 2025, 20:22 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOCreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/mpa"
      ]
    },
    {
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "mpa.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:DescribeRegisteredRegions",
```

```
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "sso:ListInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

MultiPartyApprovalReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura all'approvazione multipartitica. Questa policy include anche le relative autorizzazioni di lettura per AWS Organizations e AWS IAM Identity for approval team e fonti di identità.

`MultiPartyApprovalReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `MultiPartyApprovalReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 giugno 2025, 20:07 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalReadOnlyAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:Get*",
        "mpa:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

NeptuneConsoleFullAccess

Descrizione: fornisce l'accesso completo per gestire Amazon Neptune utilizzando. Console di gestione AWS Tieni presente che questa policy garantisce anche l'accesso completo alla pubblicazione su tutti gli argomenti SNS all'interno dell'account, le autorizzazioni per creare e modificare istanze Amazon EC2 e configurazioni VPC, le autorizzazioni per visualizzare ed elencare le chiavi su Amazon KMS e l'accesso completo ad Amazon RDS. Per ulteriori informazioni, https://aws.amazon.com/neptune/ consulta le domande frequenti/.

`NeptuneConsoleFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `NeptuneConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 giugno 2018, 21:35 UTC
- Ora modificata: 30 novembre 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
```

```
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
```

```
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
```

```
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
```

```
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:GetGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:UpdateGraph",
        "neptune-graph:ResetGraph",
```

```
        "neptune-graph:CreateGraphSnapshot",
        "neptune-graph:DeleteGraphSnapshot",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:RestoreGraphFromSnapshot",
        "neptune-graph:CreatePrivateGraphEndpoint",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:DeletePrivateGraphEndpoint",
        "neptune-graph:CreateGraphUsingImportTask",
        "neptune-graph:GetImportTask",
        "neptune-graph:ListImportTasks",
        "neptune-graph:CancelImportTask"
      ],
      "Resource" : [
        "arn:aws:neptune-graph:*:*:*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "neptune-graph.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "neptune-graph.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

NeptuneFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Neptune. Tieni presente che questa politica garantisce anche l'accesso completo alla pubblicazione su tutti gli argomenti SNS all'interno dell'account e l'accesso completo ad Amazon RDS. Per ulteriori informazioni, consulta le domande frequenti/. https://aws.amazon.com/neptune/

`NeptuneFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `NeptuneFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 maggio 2018, 19:17 UTC
- Ora modificata: 22 gennaio 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterEndpoint",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
```

```
        "rds:DeleteDBClusterEndpoint",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:FailoverGlobalCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
```

```
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:StartDBCluster",
        "rds:StopDBCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDataAccessForNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

NeptuneGraphReadOnlyAccess

Descrizione: fornisce accesso in sola lettura a tutte le risorse di Amazon Neptune Analytics insieme alle autorizzazioni di sola lettura per i servizi dipendenti.

`NeptuneGraphReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `NeptuneGraphReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 novembre 2023, 07:32 UTC
- Ora modificata: 30 novembre 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneGraph",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:Get*",
        "neptune-graph:List*",
```

```
        "neptune-graph:Read*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

NeptuneReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon Neptune. Tieni presente che questa politica consente anche l'accesso alle risorse Amazon RDS. Per ulteriori informazioni, consulta https://aws.amazon.com/neptune/ le domande frequenti/.

`NeptuneReadOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `NeptuneReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 maggio 2018, 19:16 UTC
- Ora modificata: 22 gennaio 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneDB",
      "Effect" : "Allow",
      "Action" : [
```

```
        "neptune-db:Read*",
        "neptune-db:Get*",
        "neptune-db:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

NetworkAdministrator

Descrizione: concede le autorizzazioni di accesso completo ai AWS servizi e alle azioni necessarie per impostare e configurare le risorse di AWS rete.

`NetworkAdministrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `NetworkAdministrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:31 UTC
- Ora modificata: 09 luglio 2026, 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Versione della politica

Versione della politica: v16 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDefaultNetworkAdminActions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
```

```
            "ec2:CreateInternetGateway",
            "ec2:CreateNatGateway",
            "ec2:CreateNetworkAcl",
            "ec2:CreateNetworkAclEntry",
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:CreatePlacementGroup",
            "ec2:CreateRoute",
            "ec2:CreateRouteTable",
            "ec2:CreateSecurityGroup",
            "ec2:CreateSubnet",
            "ec2:CreateTags",
            "ec2:CreateVpc",
            "ec2:CreateVpcEndpoint",
            "ec2:CreateVpcEndpointConnectionNotification",
            "ec2:CreateVpcEndpointServiceConfiguration",
            "ec2:CreateVpnConnection",
            "ec2:CreateVpnConnectionRoute",
            "ec2:CreateVpnGateway",
            "ec2:DeleteCarrierGateway",
            "ec2:DeleteEgressOnlyInternetGateway",
            "ec2:DeleteFlowLogs",
            "ec2:DeleteNatGateway",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DeletePlacementGroup",
            "ec2:DeleteSubnet",
            "ec2:DeleteTags",
            "ec2:DeleteVpc",
            "ec2:DeleteVpcEndpointConnectionNotifications",
            "ec2:DeleteVpcEndpointServiceConfigurations",
            "ec2:DeleteVpcEndpoints",
            "ec2:DeleteVpnConnection",
            "ec2:DeleteVpnConnectionRoute",
            "ec2:DeleteVpnGateway",
            "ec2:DescribeAccountAttributes",
            "ec2:DescribeAddresses",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeCarrierGateways",
            "ec2:DescribeClassicLinkInstances",
            "ec2:DescribeCustomerGateways",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeEgressOnlyInternetGateways",
            "ec2:DescribeFlowLogs",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLinkDnsSupport",
```

```
        "ec2:GetVpnConnectionDeviceSampleConfiguration",
        "ec2:GetVpnConnectionDeviceTypes",
        "ec2:GetVpnTunnelReplacementStatus",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:ModifyVpnConnection",
        "ec2:ModifyVpnConnectionOptions",
        "ec2:ModifyVpnTunnelCertificate",
        "ec2:ModifyVpnTunnelOptions",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ReplaceVpnTunnel",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:*",
        "interconnect:AcceptConnectionProposal",
        "interconnect:CreateConnection",
        "interconnect:DeleteConnection",
        "interconnect:DescribeConnectionProposal",
        "interconnect:GetConnection",
        "interconnect:GetEnvironment",
        "interconnect:ListAttachPoints",
        "interconnect:ListConnections",
```

```
        "interconnect:ListEnvironments",
        "interconnect:ListTagsForResource",
        "interconnect:TagResource",
        "interconnect:UntagResource",
        "interconnect:UpdateConnection",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "route53:*",
        "route53domains:*",
        "sns:CreateTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowVPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AssociateSecurityGroupVpc",
        "ec2:AttachClassicLinkVpc",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DetachClassicLinkVpc",
        "ec2:DisableVpcClassicLink",
        "ec2:DisassociateSecurityGroupVpc",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:RejectVpcPeeringConnection",
```

```
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowLocalGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLocalGatewayRoute",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteLocalGatewayRoute",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:SearchLocalGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DiscoverBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DiscoverFlowLogRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/flow-logs-*"
    },
    {
      "Sid" : "NetworkmanagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransitGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ExportTransitGatewayRoutes",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowTransitGatewaySLRCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

NetworkSecurityDirectorServiceLinkedRolePolicy

Descrizione: fornisce le autorizzazioni per il ruolo collegato al servizio AWS Shield Network Security Director per valutare ambienti specifici.

`NetworkSecurityDirectorServiceLinkedRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 13 giugno 2025, 20:07 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityDirectorServiceLinkedRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceLevelPermissionNotSupported",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
```

```
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetManagedPrefixListEntries",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "wafv2:ListWebACLs",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "cloudfront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "classicWaf",
      "Effect" : "Allow",
      "Action" : [
        "waf:ListWebACLs",
        "waf:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*"
      ]
```

```
    },
    {
      "Sid" : "wafv2",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:GetRuleGroup",
        "wafv2:DescribeManagedRuleGroup",
        "wafv2:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/webacl/*/*",
        "arn:aws:wafv2:*:*:regional/webacl/*/*",
        "arn:aws:apprunner:*:*:service/*",
        "arn:aws:cognito-idp:*:*:userpool/*",
        "arn:aws:ec2:*:*:verified-access-instance/*"
      ]
    },
    {
      "Sid" : "directconnect",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways"
      ],
      "Resource" : [
        "arn:aws:directconnect::*:dx-gateway/*",
        "arn:aws:directconnect:*:*:dxcon/*",
        "arn:aws:directconnect:*:*:dxlag/*",
        "arn:aws:directconnect:*:*:dxvif/*"
      ]
    },
    {
      "Sid" : "ec2Get",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ]
    },
    {
      "Sid" : "networkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListFirewalls",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*/*"
      ]
    },
    {
      "Sid" : "apiGatewayGetAPI",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AllowOrganizationsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
```

```
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "network-security-director.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccountInformationRead",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderList",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowConfigRecorderScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "config:ConfigurationRecorderServicePrincipal" : [
            "network-security-director.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

NovaActServiceRolePolicy

Descrizione: Questa politica consente di NovaAct creare e gestire le risorse necessarie per il funzionamento degli agenti Nova Act.

`NovaActServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 26 novembre 2025, 16:19 UTC
- Ora modificata: 26 novembre 2025, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NovaActServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NovaAct"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

OAMFullAccess

Descrizione: fornisce l'accesso completo a CloudWatch Observability Access Manager

`OAMFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `OAMFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 13:38 UTC
- Ora modificata: 27 novembre 2022, 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

OAMReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a CloudWatch Observability Access Manager

`OAMReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `OAMReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2022, 13:29 UTC
- Ora modificata: 27 novembre 2022, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

OpensearchIngestionSelfManagedVpcePolicy

Descrizione: consente ad Amazon OpenSearch Ingestion di descrivere le risorse di rete e scrivere metriche di servizio su cloudwatch

`OpensearchIngestionSelfManagedVpcePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 10 giugno 2024, 19:59 UTC
- Ora modificata: 10 giugno 2024, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CwPermissionsForOsiNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

PartnerCentralAccountManagementUserRoleAssociation

Descrizione: fornisce l'accesso per associare e dissociare gli utenti di Partner Central con ruoli IAM

`PartnerCentralAccountManagementUserRoleAssociation`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `PartnerCentralAccountManagementUserRoleAssociation` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 novembre 2023, 02:03 UTC
- Ora modificata: 10 novembre 2023, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "partnercentral-account-management:AssociatePartnerUser",
        "partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

PartnerCentralIncentiveBenefitManagement

Descrizione: la policy fornisce l'accesso per gestire tutti i vantaggi degli incentivi in AWS Partner Central.

`PartnerCentralIncentiveBenefitManagement`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `PartnerCentralIncentiveBenefitManagement` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 11 febbraio 2026, 16:42 UTC
- Ora modificata: 12 marzo 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralIncentiveBenefitManagement`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BenefitsManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListBenefits",
        "partnercentral:GetBenefit",
        "partnercentral:CreateBenefitApplication",
        "partnercentral:AmendBenefitApplication",
        "partnercentral:UpdateBenefitApplication",
        "partnercentral:SubmitBenefitApplication",
        "partnercentral:GetBenefitApplication",
        "partnercentral:CancelBenefitApplication",
        "partnercentral:RecallBenefitApplication",
        "partnercentral:ListBenefitApplications",
        "partnercentral:AssociateBenefitApplicationResource",
        "partnercentral:DisassociateBenefitApplicationResource",
        "partnercentral:ListBenefitAllocations",
        "partnercentral:GetBenefitAllocation"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/benefit-application/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit-allocation/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralBenefitsTaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/benefit-application/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit-allocation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AWSPartnerOpportunityAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetOpportunity",
        "partnercentral:ListOpportunities"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOffersAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

PowerUserAccess

Descrizione: fornisce l'accesso completo ai AWS servizi e alle risorse, ma non consente la gestione di utenti e gruppi.

`PowerUserAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `PowerUserAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetPrimaryEmail",
        "account:ListRegions",
        "iam:CreateServiceLinkedRole",
        "iam:DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

PricingPlanManagerFullAccess

Descrizione: fornisce l'accesso completo a AWS Pricing Plan Manager

`PricingPlanManagerFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `PricingPlanManagerFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 luglio 2026, 16:42 UTC
- Ora modificata: 30 luglio 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/PricingPlanManagerFullAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ppmglobalactions",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:CreateSubscription",
        "pricingplanmanager:ApprovePaidSubscription",
        "pricingplanmanager:UpdateSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange",
        "pricingplanmanager:AssociateResourcesToSubscription",
        "pricingplanmanager:DisassociateResourcesFromSubscription",
        "freetier:GetAccountPlanState",
        "cloudwatch:GetMetricData",
        "shield:ListProtections"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

PricingPlanManagerReadonlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS Pricing Plan Manager

`PricingPlanManagerReadonlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `PricingPlanManagerReadonlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 luglio 2026, 16:42 UTC
- Ora modificata: 30 luglio 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/PricingPlanManagerReadonlyAccess`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ppmglobalactions",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

QAppsServiceRolePolicy

Descrizione: concede autorizzazioni Servizi AWS e risorse utilizzate o gestite da Amazon Q Apps.

`QAppsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio

- Ora di creazione: 26 settembre 2024, 19:22 UTC
- Ora modificata: 26 settembre 2024, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QAppsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QAppsPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QApps"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

QBusinessQuicksightPluginPolicy

Descrizione: concede le autorizzazioni QBusiness QuickSight APIs per richiedere il plugin QuickSight

`QBusinessQuicksightPluginPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `QBusinessQuicksightPluginPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 3 dicembre 2024, 15:36 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/QBusinessQuicksightPluginPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessToQuickSightPredictQAResultsInvocation",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PredictQAResults"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:topic/*",
        "arn:aws:quicksight:*:*:dashboard/*"
```

```
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

QBusinessServiceRolePolicy

Descrizione: concede autorizzazioni Servizi AWS e risorse utilizzate o gestite da Amazon Q

`QBusinessServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 29 aprile 2024, 16:05 UTC
- Ora modificata: 29 aprile 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QBusiness"
        }
      }
    },
    {
      "Sid" : "QBusinessCreateLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QBusinessDescribeLogGroupsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "QBusinessLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

Descrizione: politica utilizzata dal QuickSight team per accedere ai dati dei clienti prodotti da S3 Storage Management Analytics.

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `QuickSightAccessForS3StorageManagementAnalyticsReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 12 giugno 2017, 18:18 UTC
- Ora modificata: 08 ottobre 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::s3-analytics-export-shared-*"
      ]
    },
    {
      "Action" : [
        "s3:GetAnalyticsConfiguration",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

RDSCloudHsmAuthorizationRole

Descrizione: policy predefinita per il ruolo del servizio Amazon RDS.

`RDSCloudHsmAuthorizationRole`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `RDSCloudHsmAuthorizationRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 26 settembre 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura a AWS servizi e risorse.

`ReadOnlyAccess`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC

- Ora modificata: 21 luglio 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Versione della politica

Versione della politica: v188 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActionsGroup1",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:GetFindingsStatistics",
        "access-analyzer:GetGeneratedPolicy",
        "access-analyzer:ListAccessPreviewFindings",
        "access-analyzer:ListAccessPreviews",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListPolicyGenerations",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetContactInformation",
```

```
        "account:GetGovCloudAccountInformation",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:SearchCertificates",
        "action-recommendations:ListRecommendedActions",
        "aidevops:DescribePrivateConnection",
        "aidevops:DescribeServices",
        "aidevops:GetAccountUsage",
        "aidevops:GetAgentSpace",
        "aidevops:GetAssociation",
        "aidevops:GetBacklogTask",
        "aidevops:GetKnowledgeItem",
        "aidevops:GetOperatorApp",
        "aidevops:GetRecommendation",
        "aidevops:GetService",
        "aidevops:ListAgentSpaces",
        "aidevops:ListAssociations",
        "aidevops:ListBacklogTasks",
        "aidevops:ListChats",
        "aidevops:ListExecutions",
        "aidevops:ListGoals",
        "aidevops:ListJournalRecords",
        "aidevops:ListKnowledgeItems",
        "aidevops:ListKnowledgeItemVersions",
        "aidevops:ListPendingMessages",
        "aidevops:ListPrivateConnections",
        "aidevops:ListRecommendations",
        "aidevops:ListServices",
        "aidevops:ListTagsForResource",
        "aidevops:ListWebhooks",
        "aidevops:SearchServiceAccessibleResource",
        "aiops:GetEphemeralInvestigationResults",
        "aiops:GetFact",
        "aiops:GetFactVersions",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationEvent",
        "aiops:GetInvestigationGroup",
```

```
        "aiops:GetInvestigationResource",
        "aiops:GetReport",
        "aiops:ListFacts",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "aiops:ValidateInvestigationGroup",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBackendEnvironment",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:GetJob",
        "amplify:GetWebhook",
        "amplify:ListApps",
        "amplify:ListArtifacts",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListJobs",
        "amplify:ListTagsForResource",
        "amplify:ListWebhooks",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetAccountSettings",
        "aoss:GetPoliciesStats",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "apigateway:GetPortal",
        "apigateway:GetPortalProduct",
        "apigateway:GetProductPage",
```

```
        "apigateway:GetProductRestEndpointPage",
        "apigateway:GetRoutingRule",
        "apigateway:ListPortalProducts",
        "apigateway:ListPortals",
        "apigateway:ListProductPages",
        "apigateway:ListProductRestEndpointPages",
        "apigateway:ListRoutingRules",
        "appconfig:GetApplication",
        "appconfig:GetConfiguration",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource",
        "appflow:DescribeConnector",
        "appflow:DescribeConnectorEntity",
        "appflow:DescribeConnectorFields",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeConnectors",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:DescribeFlows",
        "appflow:ListConnectorEntities",
        "appflow:ListConnectorFields",
        "appflow:ListConnectors",
```

```
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "application-autoscaling:GetPredictiveScalingForecast",
        "application-autoscaling:ListTagsForResource",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListAuditFindings",
        "application-signals:ListEntityEvents",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListObservedEntities",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListServiceStates",
        "application-signals:ListTagsForResource",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListServicesForAutoScalingConfiguration",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:Describe*",
        "appstream:List*",
        "appstudio:GetAccountStatus",
```

```
        "appstudio:GetEnablementJobStatus",
        "appsync:Get*",
        "appsync:List*",
        "apptest:GetTestCase",
        "apptest:GetTestConfiguration",
        "apptest:GetTestRunStep",
        "apptest:GetTestSuite",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "apptest:ListTestConfigurations",
        "apptest:ListTestRuns",
        "apptest:ListTestRunSteps",
        "apptest:ListTestRunTestCases",
        "apptest:ListTestSuites",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeAnomalyDetector",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetDefaultScraperConfiguration",
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
        "aps:ListAlertManagerSilences",
        "aps:ListAlerts",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:PreviewAnomalyDetector",
        "aps:QueryMetrics",
        "arc-region-switch:GetPlan",
```

```
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListRoute53HealthChecksInRegion",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListAutoshifts",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts",
        "artifact:GetCustomerAgreement",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements",
        "artifact:ListReports",
        "artifact:ListReportVersions",
        "athena:Batch*",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetAssessmentReportUrl",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetControl",
        "auditmanager:GetDelegations",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:GetOrganizationAdminAccount",
        "auditmanager:GetServicesInScope",
        "auditmanager:GetSettings",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
```

```
        "auditmanager:ListControls",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "auditmanager:ValidateAssessmentReportIntegrity",
        "autoscaling-plans:Describe*",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "aws-portal:View*",
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:GetVirtualMachine",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bedrock-agentcore:GetABTest",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBatchEvaluation",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetBrowserSession",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetCodeInterpreterSession",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetConfigurationBundleVersion",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetEvent",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetHarness",
        "bedrock-agentcore:GetHarnessEndpoint",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetMemoryRecord",
```

```
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetRecommendation",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListABTests",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListAgentRuntimeVersions",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBatchEvaluations",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListBrowserSessions",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListCodeInterpreterSessions",
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListConfigurationBundleVersions",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListEvents",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListHarnesses",
        "bedrock-agentcore:ListHarnessEndpoints",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListMemoryRecords",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyGenerationAssets",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListRecommendations",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock-agentcore:RetrieveMemoryRecords",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
```

```
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPrompt",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetResourcePolicy",
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModelAgreementOffers",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "billing:GetBillingData",
```

```
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetCreditAllocationHistory",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetResourcePolicy",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroupCostReports",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "braket:SearchSpendingLimits",
        "budgets:Describe*",
        "budgets:ListTagsForResource",
        "budgets:View*",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:DescribeNotificationSubscription",
        "ce:DescribeReport",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetApproximateUsageRecords",
        "ce:GetCommitmentPurchaseAnalysis",
```

```
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostComparisonDrivers",
        "ce:GetCostForecast",
        "ce:GetDimensionValues",
        "ce:GetPreferences",
        "ce:GetReservationCoverage",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetReservationUtilization",
        "ce:GetRightsizingRecommendation",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce:ListCommitmentPurchaseAnalyses",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListCostCategoryResourceAssociations",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListTagsForResource",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:List*",
        "chime:Get*",
        "chime:List*",
        "chime:Retrieve*",
        "chime:Search*",
        "chime:Validate*",
        "cleanrooms-ml:GetAudienceGenerationJob",
        "cleanrooms-ml:GetAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModelPolicy",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListAudienceExportJobs",
        "cleanrooms-ml:ListAudienceGenerationJobs",
        "cleanrooms-ml:ListAudienceModels",
        "cleanrooms-ml:ListConfiguredAudienceModels",
        "cleanrooms-ml:ListTagsForResource",
```

```
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationChangeRequest",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedJob",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationChangeRequests",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListProtectedJobs",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
```

```
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:Describe*",
        "cloudformation:Detect*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudhsm:Describe*",
        "cloudhsm:GetResourcePolicy",
        "cloudhsm:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackage",
        "codeartifact:DescribePackageVersion",
        "codeartifact:DescribeRepository",
        "codeartifact:GetAuthorizationToken",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetPackageVersionAsset",
        "codeartifact:GetPackageVersionReadme",
        "codeartifact:GetRepositoryEndpoint",
```

```
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersionAssets",
        "codeartifact:ListPackageVersionDependencies",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListRepositoriesInDomain",
        "codeartifact:ListTagsForResource",
        "codeartifact:ReadFromRepository",
        "codebuild:BatchGet*",
        "codebuild:DescribeCodeCoverages",
        "codebuild:DescribeTestCases",
        "codebuild:List*",
        "codecatalyst:GetBillingAuthorization",
        "codecatalyst:GetConnection",
        "codecatalyst:GetPendingConnection",
        "codecatalyst:ListConnections",
        "codecatalyst:ListIamRolesForConnection",
        "codecatalyst:ListTagsForResource",
        "codecommit:BatchGet*",
        "codecommit:Describe*",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:List*",
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codeconnections:GetRepositoryLink",
        "codeconnections:GetRepositorySyncStatus",
        "codeconnections:GetResourceSyncStatus",
        "codeconnections:GetSyncConfiguration",
        "codeconnections:ListConnections",
        "codeconnections:ListHosts",
        "codeconnections:ListRepositoryLinks",
        "codeconnections:ListRepositorySyncDefinitions",
        "codeconnections:ListSyncConfigurations",
        "codeconnections:ListTagsForResource",
        "codedeploy:BatchGet*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
```

```
        "codeguru-reviewer:Get*",
        "codeguru-reviewer:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetRepositorySyncStatus",
        "codestar-connections:GetResourceSyncStatus",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListRepositorySyncDefinitions",
        "codestar-connections:ListSyncConfigurations",
        "codestar-connections:ListTagsForResource",
        "codestar-notifications:describeNotificationRule",
        "codestar-notifications:listEventTypes",
        "codestar-notifications:listNotificationRules",
        "codestar-notifications:listTagsForResource",
        "codestar-notifications:ListTargets",
        "codestar:Describe*",
        "codestar:Get*",
        "codestar:List*",
        "codestar:Verify*",
        "codewhisperer:ListProfiles",
        "cognito-identity:Describe*",
        "cognito-identity:GetCredentialsForIdentity",
        "cognito-identity:GetIdentityPoolAnalytics",
        "cognito-identity:GetIdentityPoolDailyAnalytics",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetIdentityProviderDailyAnalytics",
        "cognito-identity:GetOpenIdToken",
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:List*",
        "cognito-identity:Lookup*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:Describe*",
        "cognito-idp:Get*",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
```

```
        "cognito-sync:QueryRecords",
        "comprehend:BatchDetect*",
        "comprehend:Classify*",
        "comprehend:Contains*",
        "comprehend:Describe*",
        "comprehend:Detect*",
        "comprehend:List*",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetIdleRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetRecommendationSummaries",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:Describe*",
        "connect:GetContactAttributes",
        "connect:GetCurrentMetricData",
        "connect:GetCurrentUserData",
        "connect:GetFederationToken",
        "connect:GetMetricData",
        "connect:GetMetricDataV2",
        "connect:GetTaskTemplate",
        "connect:GetTrafficDistribution",
        "connect:List*",
        "consoleapp:GetDeviceIdentity",
        "consoleapp:ListDeviceIdentities",
```

```
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "controlcatalog:GetControl",
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListControlMappings",
        "controlcatalog:ListControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEfficiencyMetrics",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "dataexchange:Get*",
        "dataexchange:List*",
        "datapipeline:Describe*",
        "datapipeline:EvaluateExpression",
        "datapipeline:Get*",
        "datapipeline:List*",
        "datapipeline:QueryObjects",
        "datapipeline:Validate*",
        "datasync:Describe*",
```

```
        "datasync:List*",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainSharingPolicy",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetProjectProfile",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
```

```
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjectProfiles",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptions",
        "datazone:ListSubscriptionTargets",
        "datazone:ListTagsForResource",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "dax:BatchGetItem",
        "dax:Describe*",
        "dax:GetItem",
        "dax:ListTags",
        "dax:Query",
        "dax:Scan",
        "deadline:BatchGetJobEntity",
        "deadline:GetApplicationVersion",
        "deadline:GetBudget",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetLicenseEndpoint",
        "deadline:GetLimit",
        "deadline:GetMonitor",
        "deadline:GetMonitorSettings",
        "deadline:GetQueue",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
```

```
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetVolume",
        "deadline:GetWorker",
        "deadline:ListAvailableMeteredProducts",
        "deadline:ListBudgets",
        "deadline:ListFarmMembers",
        "deadline:ListFarms",
        "deadline:ListFleetMembers",
        "deadline:ListFleets",
        "deadline:ListJobMembers",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListJobs",
        "deadline:ListLicenseEndpoints",
        "deadline:ListLimits",
        "deadline:ListMeteredProducts",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueueMembers",
        "deadline:ListQueues",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTagsForResource",
        "deadline:ListTasks",
        "deadline:ListVolumes",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers",
        "deepcomposer:GetComposition",
        "deepcomposer:GetModel",
        "deepcomposer:GetSampleModel",
        "deepcomposer:ListCompositions",
        "deepcomposer:ListModels",
        "deepcomposer:ListSampleModels",
```

```
        "deepcomposer:ListTrainingTopics",
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:Get*",
        "detective:List*",
        "detective:SearchGraph",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:Get*",
        "discovery:List*",
        "dlm:Get*",
        "dms:Describe*",
        "dms:List*",
        "dms:Test*",
        "docdb-elastic:GetCluster",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListPendingMaintenanceActions",
```

```
        "docdb-elastic:ListTagsForResource",
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeLaunchConfigurationTemplates",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceNetworks",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListLaunchActions",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetStream",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListStreams",
        "dsql:ListTagsForResource",
        "dynamodb:BatchGet*",
        "dynamodb:Describe*",
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "dynamodb:Scan",
        "ec2:Describe*",
        "ec2:DescribeInstanceImageMetadata",
        "ec2:Get*",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ec2messages:Get*",
        "ecr-public:BatchCheckLayerAvailability",
```

```
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetAuthorizationToken",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchCheck*",
        "ecr:BatchGet*",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:GetTaskProtection",
        "ecs:List*",
        "eks:AccessKubernetesApi",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:Request*",
        "elasticbeanstalk:Retrieve*",
        "elasticbeanstalk:Validate*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:List*",
        "elasticmapreduce:View*",
        "elastictranscoder:List*",
        "elastictranscoder:Read*",
        "elemental-appliances-software:Get*",
        "elemental-appliances-software:List*",
        "elemental-inference:ExportDictionaryEntries",
        "elemental-inference:GetDictionary",
        "elemental-inference:GetFeed",
        "elemental-inference:ListDictionaries",
        "elemental-inference:ListFeeds",
```

```
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "es:Describe*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "es:Get*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "events:Test*",
        "evidently:GetExperiment",
        "evidently:GetExperimentResults",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegmentReferences",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "evidently:TestSegmentPattern",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetAction",
        "fis:GetExperiment",
        "fis:GetExperimentTargetAccountConfiguration",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:GetTargetResourceType",
        "fis:ListActions",
```

```
        "fis:ListExperimentResolvedTargets",
        "fis:ListExperiments",
        "fis:ListExperimentTargetAccountConfigurations",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fis:ListTargetResourceTypes",
        "fms:GetAdminAccount",
        "fms:GetAdminScope",
        "fms:GetAppsList",
        "fms:GetComplianceDetail",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetProtectionStatus",
        "fms:GetProtocolsList",
        "fms:GetViolationDetails",
        "fms:ListAppsLists",
        "fms:ListComplianceStatus",
        "fms:ListMemberAccounts",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "fms:ListTagsForResource",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeExplainability",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribeMonitor",
        "forecast:DescribePredictor",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:DescribeWhatIfAnalysis",
        "forecast:DescribeWhatIfForecast",
        "forecast:DescribeWhatIfForecastExport",
        "forecast:GetAccuracyMetrics",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListExplainabilities",
        "forecast:ListExplainabilityExports",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
```

```
        "forecast:ListMonitorEvaluations",
        "forecast:ListMonitors",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "forecast:ListWhatIfAnalyses",
        "forecast:ListWhatIfForecastExports",
        "forecast:ListWhatIfForecasts",
        "forecast:QueryForecast",
        "forecast:QueryWhatIfForecast",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:DescribeModelVersions",
        "frauddetector:GetBatchImportJobs",
        "frauddetector:GetBatchPredictionJobs",
        "frauddetector:GetDeleteEventsByEventTypeStatus",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEvent",
        "frauddetector:GetEventPredictionMetadata",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListEventPredictions",
        "frauddetector:ListTagsForResource",
        "freertos:Describe*",
        "freertos:List*",
        "freetier:GetAccountActivity",
        "freetier:GetAccountPlanState",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:ListAccountActivities",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:Describe*",
        "gamelift:Get*",
```

```
        "gamelift:List*",
        "gamelift:ResolveAlias",
        "gamelift:Search*",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListStreamSessions",
        "gameliftstreams:ListStreamSessionsByAccount",
        "gameliftstreams:ListTagsForResource",
        "glacier:Describe*",
        "glacier:Get*",
        "glacier:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetCrawlers",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:BatchGetTriggers",
        "glue:BatchGetWorkflows",
        "glue:CheckSchemaVersionValidity",
        "glue:GetCatalog",
        "glue:GetCatalogImportStatus",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDataflowGraph",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetMapping",
        "glue:GetMLTaskRun",
```

```
        "glue:GetMLTaskRuns",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetPlan",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetTriggers",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:GetWorkflowRunProperties",
        "glue:GetWorkflowRuns",
        "glue:ListCrawlers",
        "glue:ListCrawls",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSchemas",
        "glue:ListSchemaVersions",
        "glue:ListSessions",
        "glue:ListStatements",
        "glue:ListTableOptimizerRuns",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "glue:QuerySchemaVersionMetadata",
```

```
        "glue:SearchTables",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListPermissions",
        "grafana:ListTagsForResource",
        "grafana:ListVersions",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:Get*",
        "greengrass:List*",
        "groundstation:DescribeContactVersion",
        "groundstation:DescribeEphemeris",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMinuteUsage",
        "groundstation:GetMissionProfile",
        "groundstation:GetSatellite",
        "groundstation:ListAntennas",
        "groundstation:ListConfigs",
        "groundstation:ListContacts",
        "groundstation:ListContactVersions",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListEphemerides",
        "groundstation:ListGroundStationReservations",
        "groundstation:ListGroundStations",
        "groundstation:ListMissionProfiles",
        "groundstation:ListSatellites",
        "groundstation:ListTagsForResource",
        "groundstation:DescribeContact",
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:GetCapabilities",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListFHIRExportJobs",
        "healthlake:ListFHIRImportJobs",
        "healthlake:ListTagsForResource",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
```

```
        "healthlake:SearchWithPost",
        "iam:Generate*",
        "iam:Get*",
        "iam:List*",
        "iam:Simulate*",
        "identity-sync:GetSyncProfile",
        "identity-sync:GetSyncTarget",
        "identity-sync:ListSyncFilters",
        "identitystore-auth:BatchGetSession",
        "identitystore-auth:ListSessions",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "importexport:Get*",
        "importexport:List*",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetCodeSnippet",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:BatchGetMemberEc2DeepInspectionStatus",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetCisScanReport",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetEc2DeepInspectionConfiguration",
        "inspector2:GetEncryptionKey",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:GetSbomExport",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCisScanConfigurations",
```

```
        "inspector2:ListCisScans",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "inspector2:SearchVulnerabilities",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "interconnect:DescribeConnectionProposal",
        "interconnect:GetConnection",
        "interconnect:GetEnvironment",
        "interconnect:ListAttachPoints",
        "interconnect:ListTagsForResource",
        "interconnect:ListEnvironments",
        "interconnect:ListConnections",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
        "iot1click:ListProjects",
        "iot1click:ListTagsForResource",
        "iotanalytics:Describe*",
        "iotanalytics:Get*",
        "iotanalytics:List*",
```

```
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModels",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectors",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetLoggingOptions",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetRegisterAccountStatus",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:GetVehicleStatus",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
```

```
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless:GetMetricConfiguration",
        "iotwireless:GetMetrics",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetMulticastGroupSession",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetPosition",
        "iotwireless:GetPositionConfiguration",
        "iotwireless:GetPositionEstimate",
        "iotwireless:GetResourceEventConfiguration",
        "iotwireless:GetResourceLogLevel",
        "iotwireless:GetResourcePosition",
        "iotwireless:GetServiceEndpoint",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessDeviceStatistics",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayCertificate",
        "iotwireless:GetWirelessGatewayFirmwareInformation",
        "iotwireless:GetWirelessGatewayStatistics",
        "iotwireless:GetWirelessGatewayTask",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListEventConfigurations",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListMulticastGroupsByFuotaTask",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListPositionConfigurations",
        "iotwireless:ListQueuedMessages",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:BatchGetChannel",
```

```
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipantEvents",
        "ivs:ListParticipants",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyActionsGroup2",
      "Effect" : "Allow",
      "Action" : [
        "kafka:Describe*",
```

```
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:Get*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafka:ListClusterOperations",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurationRevisions",
        "kafka:ListConfigurations",
        "kafka:ListKafkaVersions",
        "kafka:ListNodes",
        "kafka:ListTagsForResource",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:BatchGetDocumentStatus",
        "kendra:DescribeDataSource",
        "kendra:DescribeExperience",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:DescribePrincipalMapping",
        "kendra:DescribeQuerySuggestionsBlockList",
        "kendra:DescribeQuerySuggestionsConfig",
        "kendra:DescribeThesaurus",
        "kendra:GetQuerySuggestions",
        "kendra:GetSnapshots",
        "kendra:ListDataSources",
        "kendra:ListDataSourceSyncJobs",
        "kendra:ListEntityPersonas",
        "kendra:ListExperienceEntities",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListGroupsOlderThanOrderingId",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListTagsForResource",
```

```
        "kendra:ListThesauri",
        "kendra:Query",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Discover*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetEffectivePermissionsForPath",
        "lakeformation:GetLfTag",
        "lakeformation:GetResourceLfTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLfTags",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListTableStorageOptimizers",
        "lakeformation:SearchDatabasesByLfTags",
        "lakeformation:SearchTablesByLfTags",
        "lambda:Get*",
        "lambda:List*",
        "launchwizard:DescribeAdditionalNode",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:DescribeProvisioningEvents",
        "launchwizard:DescribeSettingsSet",
        "launchwizard:GetDeployment",
        "launchwizard:GetInfrastructureSuggestion",
        "launchwizard:GetIpAddress",
        "launchwizard:GetResourceCostEstimate",
        "launchwizard:GetResourceRecommendation",
        "launchwizard:GetSettingsSet",
        "launchwizard:GetWorkload",
        "launchwizard:GetWorkloadAsset",
        "launchwizard:GetWorkloadAssets",
        "launchwizard:GetWorkloadDeploymentPattern",
```

```
        "launchwizard:ListAdditionalNodes",
        "launchwizard:ListAllowedResources",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListProvisionedApps",
        "launchwizard:ListResourceCostEstimates",
        "launchwizard:ListSettingsSets",
        "launchwizard:ListTagsForResource",
        "launchwizard:ListWorkloadDeploymentOptions",
        "launchwizard:ListWorkloadDeploymentPatterns",
        "launchwizard:ListWorkloads",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:Get*",
        "lex:ListBotAliases",
        "lex:ListBotAliasReplicas",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBotReplicas",
        "lex:ListBots",
        "lex:ListBotVersionReplicas",
        "lex:ListBotVersions",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "license-manager:Get*",
        "license-manager:List*",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
```

```
        "lightsail:GetAutoSnapshots",
        "lightsail:GetBlueprints",
        "lightsail:GetBucketAccessKeys",
        "lightsail:GetBucketBundles",
        "lightsail:GetBucketMetricData",
        "lightsail:GetBuckets",
        "lightsail:GetBundles",
        "lightsail:GetCertificates",
        "lightsail:GetCloudFormationStackRecords",
        "lightsail:GetContainerAPIMetadata",
        "lightsail:GetContainerImages",
        "lightsail:GetContainerServiceDeployments",
        "lightsail:GetContainerServiceMetricData",
        "lightsail:GetContainerServicePowers",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetExportSnapshotRecords",
        "lightsail:GetInstance",
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerMetricData",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperation",
        "lightsail:GetOperations",
        "lightsail:GetOperationsForResource",
        "lightsail:GetRegions",
        "lightsail:GetRelationalDatabase",
```

```
        "lightsail:GetRelationalDatabaseBlueprints",
        "lightsail:GetRelationalDatabaseBundles",
        "lightsail:GetRelationalDatabaseEvents",
        "lightsail:GetRelationalDatabaseLogEvents",
        "lightsail:GetRelationalDatabaseLogStreams",
        "lightsail:GetRelationalDatabaseMetricData",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:Get*",
        "logs:ListAggregateLogGroupSummaries",
        "logs:ListAnomalies",
        "logs:ListEntitiesForLogGroup",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListScheduledQueries",
        "logs:ListSourcesForS3TableIntegration",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "logs:StartLiveTail",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutequipment:DescribeDataIngestionJob",
        "lookoutequipment:DescribeDataset",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:DescribeLabel",
        "lookoutequipment:DescribeLabelGroup",
        "lookoutequipment:DescribeModel",
        "lookoutequipment:DescribeModelVersion",
        "lookoutequipment:DescribeResourcePolicy",
        "lookoutequipment:DescribeRetrainingScheduler",
        "lookoutequipment:ListDataIngestionJobs",
        "lookoutequipment:ListDatasets",
```

```
        "lookoutequipment:ListInferenceEvents",
        "lookoutequipment:ListInferenceExecutions",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutequipment:ListLabelGroups",
        "lookoutequipment:ListLabels",
        "lookoutequipment:ListModels",
        "lookoutequipment:ListModelVersions",
        "lookoutequipment:ListRetrainingSchedulers",
        "lookoutequipment:ListSensorStatistics",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:Get*",
        "lookoutmetrics:List*",
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "m2:GetApplication",
        "m2:GetApplicationVersion",
        "m2:GetBatchJobExecution",
        "m2:GetDataSetDetails",
        "m2:GetDataSetImportTask",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListApplicationVersions",
        "m2:ListBatchJobDefinitions",
        "m2:ListBatchJobExecutions",
        "m2:ListDataSetImportHistory",
        "m2:ListDataSets",
        "m2:ListDeployments",
        "m2:ListEngineVersions",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:DescribeBuckets",
        "macie2:DescribeClassificationJob",
```

```
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAdministratorAccount",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetBucketStatistics",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetClassificationScope",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindings",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetFindingStatistics",
        "macie2:GetInvitationsCount",
        "macie2:GetMacieSession",
        "macie2:GetMember",
        "macie2:GetResourceProfile",
        "macie2:GetRevealConfiguration",
        "macie2:GetSensitiveDataOccurrencesAvailability",
        "macie2:GetSensitivityInspectionTemplate",
        "macie2:GetUsageStatistics",
        "macie2:GetUsageTotals",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListClassificationJobs",
        "macie2:ListClassificationScopes",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindings",
        "macie2:ListFindingsFilters",
        "macie2:ListInvitations",
        "macie2:ListMembers",
        "macie2:ListOrganizationAdminAccounts",
        "macie2:ListResourceProfileArtifacts",
        "macie2:ListResourceProfileDetections",
        "macie2:ListSensitivityInspectionTemplates",
        "macie2:ListTagsForResource",
        "macie2:SearchResources",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:GetProposal",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNetworks",
        "managedblockchain:ListNodes",
```

```
        "managedblockchain:ListProposals",
        "managedblockchain:ListProposalVotes",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeFlowSourceMetadata",
        "mediaconnect:DescribeFlowSourceThumbnail",
        "mediaconnect:DescribeGateway",
        "mediaconnect:DescribeGatewayInstance",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:GetRouterOutput",
        "mediaconnect:ListBridges",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGatewayInstances",
        "mediaconnect:ListGateways",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:Probe",
        "mediaconvert:SearchJobs",
        "medialive:DescribeAccountConfiguration",
        "medialive:DescribeChannel",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeCluster",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNetwork",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
```

```
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannels",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListInputDevices",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputs",
        "medialive:ListInputSecurityGroups",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetHeadObject",
        "mediapackagev2:GetObject",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediapackagev2:ListTagsForResource",
        "mediastore:DescribeContainer",
        "mediastore:DescribeObject",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:GetMetricPolicy",
        "mediastore:GetObject",
        "mediastore:ListContainers",
        "mediastore:ListItems",
```

```
        "mediastore:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeEngineVersions",
        "memorydb:DescribeEvents",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeMultiRegionParameterGroups",
        "memorydb:DescribeMultiRegionParameters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeReservedNodes",
        "memorydb:DescribeReservedNodesOfferings",
        "memorydb:DescribeServiceUpdates",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListAllowedMultiRegionClusterUpdates",
        "memorydb:ListAllowedNodeTypeUpdates",
        "memorydb:ListTags",
        "mgh:Describe*",
        "mgh:GetHomeRegion",
        "mgh:List*",
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:GetReplicationConfiguration",
        "mgn:ListApplications",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListWaves",
        "mobileanalytics:Get*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "monitron:GetProject",
        "monitron:GetProjectAdminUser",
        "monitron:ListProjects",
        "monitron:ListTagsForResource",
        "mpa:GetApprovalTeam",
        "mpa:GetIdentitySource",
        "mpa:GetPolicyVersion",
```

```
        "mpa:GetResourcePolicy",
        "mpa:GetSession",
        "mpa:ListApprovalTeams",
        "mpa:ListIdentitySources",
        "mpa:ListPolicies",
        "mpa:ListPolicyVersions",
        "mpa:ListResourcePolicies",
        "mpa:ListSessions",
        "mpa:ListTagsForResource",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeProxy",
        "network-firewall:DescribeProxyConfiguration",
        "network-firewall:DescribeProxyRule",
        "network-firewall:DescribeProxyRuleGroup",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListProxies",
        "network-firewall:ListProxyConfigurations",
        "network-firewall:ListProxyRuleGroups",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "networkflowmonitor:GetMonitor",
        "networkflowmonitor:GetScope",
        "networkflowmonitor:ListMonitors",
        "networkflowmonitor:ListScopes",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnections",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkChangeEvents",
        "networkmanager:GetCoreNetworkChangeSet",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
```

```
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetNetworkResourceCounts",
        "networkmanager:GetNetworkResourceRelationships",
        "networkmanager:GetNetworkResources",
        "networkmanager:GetNetworkRoutes",
        "networkmanager:GetNetworkTelemetry",
        "networkmanager:GetResourcePolicy",
        "networkmanager:GetRouteAnalysis",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachmentRoutingPolicyAssociations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
        "networkmanager:ListCoreNetworkPrefixListAssociations",
        "networkmanager:ListCoreNetworkRoutingInformation",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "networkmonitor:GetMonitor",
        "networkmonitor:GetProbe",
        "networkmonitor:ListMonitors",
        "networkmonitor:ListTagsForResource",
        "nimble:GetEula",
        "nimble:GetFeatureMap",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileMember",
        "nimble:GetStreamingImage",
        "nimble:GetStreamingSession",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:GetStudioMember",
        "nimble:ListEulaAcceptances",
        "nimble:ListEulas",
        "nimble:ListLaunchProfileMembers",
```

```
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStreamingSessions",
        "nimble:ListStudioComponents",
        "nimble:ListStudioMembers",
        "nimble:ListStudios",
        "nimble:ListTagsForResource",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:GetFeatureOptInStatus",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "omics:Get*",
```

```
        "omics:List*",
        "one:GetDeviceConfigurationTemplate",
        "one:GetDeviceInstance",
        "one:GetDeviceInstanceConfiguration",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceConfigurationTemplates",
        "one:ListDeviceInstances",
        "one:ListSites",
        "one:ListUsers",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:GetPipelineBlueprint",
        "osis:GetPipelineChangeProgress",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:Get*",
        "outposts:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetPublicKeyCertificate",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
```

```
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:Describe*",
        "personalize:Get*",
        "personalize:List*",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "polly:Describe*",
        "polly:Get*",
        "polly:List*",
        "polly:SynthesizeSpeech",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetPriceListFileUrl",
        "pricing:GetProducts",
        "pricing:ListPriceLists",
        "proton:GetDeployment",
        "proton:GetEnvironment",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
```

```
        "proton:GetServiceTemplateVersion",
        "proton:ListDeployments",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceInstances",
        "proton:ListServices",
        "proton:ListServiceTemplates",
        "proton:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ViewPurchaseOrders",
        "qbusiness:GetApplication",
        "qbusiness:GetChatControlsConfiguration",
        "qbusiness:GetDataSource",
        "qbusiness:GetGroup",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetUser",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListDataSourceSyncJobs",
        "qbusiness:ListGroups",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalKinesisStream",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "qldb:ListTagsForResource",
        "ram:Get*",
```

```
        "ram:List*",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:Describe*",
        "rds:Download*",
        "rds:List*",
        "redshift-serverless:GetCustomDomainAssociation",
        "redshift-serverless:GetEndpointAccess",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetRecoveryPoint",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:GetScheduledAction",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetTableRestoreStatus",
        "redshift-serverless:GetUsageLimit",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListCustomDomainAssociations",
        "redshift-serverless:ListEndpointAccess",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListRecoveryPoints",
        "redshift-serverless:ListScheduledActions",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTableRestoreStatus",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListUsageLimits",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
        "redshift:ListRecommendations",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
```

```
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeStreamProcessor",
        "rekognition:Detect*",
        "rekognition:GetCelebrityInfo",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetContentModeration",
        "rekognition:GetFaceDetection",
        "rekognition:GetFaceSearch",
        "rekognition:GetLabelDetection",
        "rekognition:GetPersonTracking",
        "rekognition:GetSegmentDetection",
        "rekognition:GetTextDetection",
        "rekognition:List*",
        "rekognition:RecognizeCelebrities",
        "rekognition:Search*",
        "resiliencehub:GetFailureModeFinding",
        "resiliencehub:GetPolicy",
        "resiliencehub:GetService",
        "resiliencehub:GetSystem",
        "resiliencehub:GetUserJourney",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppAssessment",
        "resiliencehub:DescribeAppVersion",
        "resiliencehub:DescribeAppVersionAppComponent",
        "resiliencehub:DescribeAppVersionResource",
        "resiliencehub:DescribeAppVersionResourcesResolutionStatus",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
        "resiliencehub:DescribeMetricsExport",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:DescribeResourceGroupingRecommendationTask",
        "resiliencehub:ListAlarmRecommendations",
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessmentResourceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
```

```
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListAssertions",
        "resiliencehub:ListDependencies",
        "resiliencehub:ListFailureModeAssessments",
        "resiliencehub:ListFailureModeFindings",
        "resiliencehub:ListInputSources",
        "resiliencehub:ListMetrics",
        "resiliencehub:ListPolicies",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListReports",
        "resiliencehub:ListResources",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListResourceGroupingRecommendations",
        "resiliencehub:ListServices",
        "resiliencehub:ListServiceEvents",
        "resiliencehub:ListServiceFunctions",
        "resiliencehub:ListServiceEvents",
        "resiliencehub:ListServiceFunctions",
        "resiliencehub:ListServiceTopologyEdges",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListSystems",
        "resiliencehub:ListSystemEvents",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resiliencehub:ListUserJourneys",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetResourceExplorerSetup",
        "resource-explorer-2:GetServiceIndex",
        "resource-explorer-2:GetServiceView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListServiceIndexes",
        "resource-explorer-2:ListServiceViews",
        "resource-explorer-2:ListStreamingAccessForServices",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
```

```
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
```

```
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListManagedFirewallDomainLists",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetBucketVersioning",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:GetObject",
        "s3-outposts:GetObjectTagging",
        "s3-outposts:GetObjectVersion",
        "s3-outposts:GetObjectVersionForReplication",
        "s3-outposts:GetObjectVersionTagging",
        "s3-outposts:GetReplicationConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListBucket",
        "s3-outposts:ListBucketMultipartUploads",
```

```
        "s3-outposts:ListBucketVersions",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListMultipartUploadParts",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListRegionalBuckets",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableData",
        "s3tables:GetTableEncryption",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTableMaintenanceJobStatus",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableRecordExpirationConfiguration",
        "s3tables:GetTableRecordExpirationJobStatus",
        "s3tables:GetTableReplication",
```

```
        "s3tables:GetTableReplicationStatus",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:GetVectors",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "sagemaker:Describe*",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:Describe*",
        "schemas:Get*",
        "schemas:List*",
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetCodeReviewJobs",
        "securityagent:BatchGetCodeReviewJobTasks",
        "securityagent:BatchGetCodeReviews",
        "securityagent:BatchGetFindings",
```

```
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentestJobTasks",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:GetArtifact",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
        "securityagent:GetDesignReviewFeedback",
        "securityagent:GetIntegration",
        "securityagent:ListAgentSpaces",
        "securityagent:ListApplications",
        "securityagent:ListArtifacts",
        "securityagent:ListCodeReviewJobsForCodeReview",
        "securityagent:ListCodeReviewJobTasks",
        "securityagent:ListCodeReviews",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListTargetDomains",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListIntegrations",
        "securityagent:ListMemberships",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListResourcesFromIntegration",
        "securityagent:ListPentestJobTasks",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "securitylake:GetDataLakeExceptionSubscription",
        "securitylake:GetDataLakeOrganizationConfiguration",
        "securitylake:GetDataLakeSources",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
```

```
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serverlessrepo:Get*",
        "serverlessrepo:List*",
        "serverlessrepo:SearchApplications",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAutoManagementConfiguration",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetQuotaUtilizationReport",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:StartQuotaUtilizationReport",
        "ses:BatchGetMetricData",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "signer:DescribeSigningJob",
        "signer:GetSigningPlatform",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningJobs",
        "signer:ListSigningPlatforms",
        "signer:ListSigningProfiles",
```

```
        "signer:ListTagsForResource",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeRegistrationAttachments",
        "sms-voice:DescribeRegistrationFieldDefinitions",
        "sms-voice:DescribeRegistrationFieldValues",
        "sms-voice:DescribeRegistrations",
        "sms-voice:DescribeRegistrationSectionDefinitions",
        "sms-voice:DescribeRegistrationTypeDefinitions",
        "sms-voice:DescribeRegistrationVersions",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
        "snowball:Get*",
        "snowball:List*",
        "sns:Check*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "sqs:Receive*",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:DescribePage",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListEngagements",
        "ssm-contacts:ListPageReceipts",
        "ssm-contacts:ListPagesByContact",
        "ssm-contacts:ListPagesByEngagement",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:GetReplicationSet",
```

```
        "ssm-incidents:GetResourcePolicies",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-incidents:ListTimelineEvents",
        "ssm-quicksetup:GetConfiguration",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:GetServiceSettings",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:ListConfigurations",
        "ssm-quicksetup:ListQuickSetupTypes",
        "ssm-quicksetup:ListTagsForResource",
        "ssm-sap:GetApplication",
        "ssm-sap:GetComponent",
        "ssm-sap:GetConfigurationCheckOperation",
        "ssm-sap:GetDatabase",
        "ssm-sap:GetOperation",
        "ssm-sap:GetResourcePermission",
        "ssm-sap:ListApplications",
        "ssm-sap:ListComponents",
        "ssm-sap:ListConfigurationCheckDefinitions",
        "ssm-sap:ListConfigurationCheckOperations",
        "ssm-sap:ListDatabases",
        "ssm-sap:ListOperationEvents",
        "ssm-sap:ListOperations",
        "ssm-sap:ListSubCheckResults",
        "ssm-sap:ListSubCheckRuleResults",
        "ssm-sap:ListTagsForResource",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
```

```
        "states:ValidateStateMachineDefinition",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "sts:GetCallerIdentity",
        "sts:GetSessionToken",
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunication",
        "support:DescribeCommunications",
        "support:DescribeCreateCaseOptions",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportedLanguages",
        "support:DescribeSupportLevel",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:SearchForCases",
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "sustainability:GetCarbonFootprintSummary",
        "sustainability:GetEstimatedCarbonEmissions",
        "sustainability:GetEstimatedCarbonEmissionsDimensionValues",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:DescribeReportCreation",
        "tag:Get*",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "timestream:DescribeBatchLoadTask",
```

```
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListBatchLoadTasks",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "tnb:GetSolFunctionInstance",
        "tnb:GetSolFunctionPackage",
        "tnb:GetSolFunctionPackageContent",
        "tnb:GetSolFunctionPackageDescriptor",
        "tnb:GetSolNetworkInstance",
        "tnb:GetSolNetworkOperation",
        "tnb:GetSolNetworkPackage",
        "tnb:GetSolNetworkPackageContent",
        "tnb:GetSolNetworkPackageDescriptor",
        "tnb:ListSolFunctionInstances",
        "tnb:ListSolFunctionPackages",
        "tnb:ListSolNetworkInstances",
        "tnb:ListSolNetworkOperations",
        "tnb:ListSolNetworkPackages",
        "tnb:ListTagsForResource",
        "transcribe:Get*",
        "transcribe:List*",
        "transfer:Describe*",
        "transfer:List*",
        "transfer:TestIdentityProvider",
        "transform:GetAccountSettings",
        "transform:GetAgent",
        "transform:GetAgentRuntimeConfiguration",
        "transform:GetConnector",
        "transform:ListAgents",
        "transform:ListConnectors",
        "transform:ListProfiles",
        "transform:ListTagsForResource",
        "transform-custom:GetAnalysis",
        "transform-custom:GetCampaign",
        "transform-custom:GetFinding",
        "transform-custom:GetFindingGroups",
        "transform-custom:GetKnowledgeItem",
        "transform-custom:GetRemediation",
        "transform-custom:GetRepository",
        "transform-custom:GetSource",
```

```
        "transform-custom:ListAnalyses",
        "transform-custom:ListCampaigns",
        "transform-custom:ListCampaignRepositories",
        "transform-custom:ListFindings",
        "transform-custom:ListKnowledgeItems",
        "transform-custom:ListRemediations",
        "transform-custom:ListRepositories",
        "transform-custom:ListSources",
        "transform-custom:ListTagsForResource",
        "transform-custom:ListTransformationPackageMetadata",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "trustedadvisor:GetOrganizationRecommendation",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListOrganizationRecommendationAccounts",
        "trustedadvisor:ListOrganizationRecommendationResources",
        "trustedadvisor:ListOrganizationRecommendations",
        "trustedadvisor:ListRecommendationResources",
        "trustedadvisor:ListRecommendations",
        "user-subscriptions:ListApplicationClaims",
        "user-subscriptions:ListClaims",
        "user-subscriptions:ListUserSubscriptions",
        "uxc:GetAccountColor",
        "uxc:GetAccountCustomizations",
        "uxc:ListServices",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
```

```
        "vpc-lattice:GetDomainVerification",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListDomainVerifications",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceEndpointAssociations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServiceNetworkVpcEndpointAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:CheckCapacity",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wellarchitected:ExportLens",
        "wellarchitected:GetAnswer",
        "wellarchitected:GetConsolidatedReport",
        "wellarchitected:GetLens",
        "wellarchitected:GetLensReview",
        "wellarchitected:GetLensReviewReport",
        "wellarchitected:GetLensVersionDifference",
        "wellarchitected:GetMilestone",
```

```
        "wellarchitected:GetProfile",
        "wellarchitected:GetProfileTemplate",
        "wellarchitected:GetReviewTemplate",
        "wellarchitected:GetReviewTemplateAnswer",
        "wellarchitected:GetReviewTemplateLensReview",
        "wellarchitected:GetWorkload",
        "wellarchitected:List*",
        "workdocs:CheckAlias",
        "workdocs:Describe*",
        "workdocs:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:Describe*",
        "xray:BatchGet*",
        "xray:CancelTraceRetrieval",
        "xray:Get*",
        "xray:ListResourcePolicies",
        "xray:ListRetrievedTraces",
        "xray:ListTagsForResource",
        "xray:StartTraceRetrieval"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ExpressReadOnlySessionObjectAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3express:SessionMode" : "ReadOnly"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ReInventTicketApprovalAccess

Descrizione: concede a un ruolo o utente IAM l'accesso completo per visualizzare i dettagli degli addebiti di re:Invent Pass e approvare la fatturazione sui propri account AWS

`ReInventTicketApprovalAccess`AWS è una politica gestita.

Utilizzo di questa politica

È possibile associare la policy `ReInventTicketApprovalAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 10 giugno 2026, 18:57 UTC
- Ora modificata: 10 giugno 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ReInventTicketApprovalAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBillToAWSActions",
      "Effect" : "Allow",
      "Action" : [
        "eventsbilltoaws:info",
        "eventsbilltoaws:approve"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ResourceGroupsandTagEditorFullAccess

Descrizione: Fornisce l'accesso completo a Resource Groups e Tag Editor.

`ResourceGroupsandTagEditorFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ResourceGroupsandTagEditorFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 10 agosto 2023, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources",
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ResourceGroupsandTagEditorReadOnlyAccess

Descrizione: Fornisce l'accesso all'utilizzo di Resource Groups e Tag Editor, ma non consente la modifica dei tag tramite il Tag Editor.

`ResourceGroupsandTagEditorReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ResourceGroupsandTagEditorReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:39 UTC
- Ora modificata: 10 agosto 2023, 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ResourceGroupsServiceRolePolicy

Descrizione: consente ai AWS Resource Groups di interrogare i AWS servizi che possiedono le tue risorse per mantenere il gruppo up-to-date

`ResourceGroupsServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 5 gennaio 2023, 16:57 UTC
- Ora modificata: 05 gennaio 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ResourceGroupsTaggingAPITagUntagSupportedResources

Descrizione: fornisce le autorizzazioni per etichettare e rimuovere i tag da tutte le risorse supportate dall'API Resource Groups Tagging. Questa politica concede anche le autorizzazioni necessarie per recuperare tutte le risorse taggate o precedentemente taggate tramite l'API Resource Groups Tagging.

`ResourceGroupsTaggingAPITagUntagSupportedResources`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `ResourceGroupsTaggingAPITagUntagSupportedResources` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 ottobre 2024, 11:11 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsTaggingAPITagUntagSupportedResources`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:TagResource",
        "a4b:UntagResource",
        "access-analyzer:TagResource",
        "access-analyzer:UntagResource",
        "acm-pca:TagCertificateAuthority",
        "acm-pca:UntagCertificateAuthority",
        "acm:AddTagsToCertificate",
        "acm:RemoveTagsFromCertificate",
        "amplify:TagResource",
        "amplify:UntagResource",
        "appconfig:TagResource",
        "appconfig:UntagResource",
        "appflow:TagResource",
        "appflow:UntagResource",
        "appmesh:TagResource",
        "appmesh:UntagResource",
        "appstream:TagResource",
        "appstream:UntagResource",
        "appsync:TagResource",
        "appsync:UntagResource",
        "athena:TagResource",
        "athena:UntagResource",
        "auditmanager:TagResource",
        "auditmanager:UntagResource",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteTags",
        "backup:TagResource",
        "backup:UntagResource",
        "batch:TagResource",
        "batch:UntagResource",
        "braket:TagResource",
        "braket:UntagResource",
        "cassandra:TagResource",
        "cassandra:UntagResource",
        "chime:TagResource",
```

```
        "chime:UntagResource",
        "cloud9:TagResource",
        "cloud9:UntagResource",
        "clouddirectory:TagResource",
        "clouddirectory:UntagResource",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudhsm:TagResource",
        "cloudhsm:UntagResource",
        "cloudtrail:AddTags",
        "cloudtrail:RemoveTags",
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource",
        "codeartifact:TagResource",
        "codeartifact:UntagResource",
        "codecommit:TagResource",
        "codecommit:UntagResource",
        "codedeploy:AddTagsToOnPremisesInstances",
        "codedeploy:RemoveTagsFromOnPremisesInstances",
        "codedeploy:TagResource",
        "codedeploy:UntagResource",
        "codeguru-profiler:TagResource",
        "codeguru-profiler:UntagResource",
        "codepipeline:TagResource",
        "codepipeline:UntagResource",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar:TagProject",
        "codestar:UntagProject",
        "cognito-identity:TagResource",
        "cognito-identity:UntagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UntagResource",
        "comprehend:TagResource",
        "comprehend:UntagResource",
        "config:TagResource",
        "config:UntagResource",
        "connect:TagResource",
        "connect:UntagResource",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "datapipeline:AddTags",
        "datapipeline:RemoveTags",
        "datasync:TagResource",
```

```
        "datasync:UntagResource",
        "deepcomposer:TagResource",
        "deepcomposer:UntagResource",
        "detective:TagResource",
        "detective:UntagResource",
        "devicefarm:TagResource",
        "devicefarm:UntagResource",
        "directconnect:TagResource",
        "directconnect:UntagResource",
        "dlm:TagResource",
        "dlm:UntagResource",
        "dms:AddTagsToResource",
        "dms:RemoveTagsFromResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ecr:TagResource",
        "ecr:UntagResource",
        "ecs:TagResource",
        "ecs:UntagResource",
        "eks:TagResource",
        "eks:UntagResource",
        "elastic-inference:TagResource",
        "elastic-inference:UntagResource",
        "elasticache:AddTagsToResource",
        "elasticache:RemoveTagsFromResource",
        "elasticbeanstalk:UpdateTagsForResource",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:DeleteTags",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "emr-containers:TagResource",
        "emr-containers:UntagResource",
        "es:AddTags",
        "es:RemoveTags",
        "events:TagResource",
        "events:UntagResource",
        "firehose:TagDeliveryStream",
        "firehose:UntagDeliveryStream",
        "fms:TagResource",
        "fms:UntagResource",
```

```
        "forecast:TagResource",
        "forecast:UntagResource",
        "frauddetector:TagResource",
        "frauddetector:UntagResource",
        "fsx:TagResource",
        "fsx:UntagResource",
        "gamelift:TagResource",
        "gamelift:UntagResource",
        "glacier:AddTagsToVault",
        "glacier:RemoveTagsFromVault",
        "globalaccelerator:TagResource",
        "globalaccelerator:UntagResource",
        "glue:TagResource",
        "glue:UntagResource",
        "greengrass:TagResource",
        "greengrass:UntagResource",
        "groundstation:TagResource",
        "groundstation:UntagResource",
        "guardduty:TagResource",
        "guardduty:UntagResource",
        "iam:TagInstanceProfile",
        "iam:TagMFADevice",
        "iam:TagOpenIDConnectProvider",
        "iam:TagPolicy",
        "iam:TagRole",
        "iam:TagSAMLProvider",
        "iam:TagServerCertificate",
        "iam:TagUser",
        "iam:UntagInstanceProfile",
        "iam:UntagMFADevice",
        "iam:UntagOpenIDConnectProvider",
        "iam:UntagPolicy",
        "iam:UntagRole",
        "iam:UntagSAMLProvider",
        "iam:UntagServerCertificate",
        "iam:UntagUser",
        "imagebuilder:TagResource",
        "imagebuilder:UntagResource",
        "inspector:ListTagsForResource",
        "inspector:SetTagsForResource",
        "iot1click:TagResource",
        "iot1click:UntagResource",
        "iot:TagResource",
        "iot:UntagResource",
```

```
        "iotanalytics:TagResource",
        "iotanalytics:UntagResource",
        "iotdeviceadvisor:TagResource",
        "iotdeviceadvisor:UntagResource",
        "iotevents:TagResource",
        "iotevents:UntagResource",
        "iotfleethub:TagResource",
        "iotfleethub:UntagResource",
        "iotsitewise:TagResource",
        "iotsitewise:UntagResource",
        "iottwinmaker:TagResource",
        "iottwinmaker:UntagResource",
        "iotwireless:TagResource",
        "iotwireless:UntagResource",
        "ivs:TagResource",
        "ivs:UntagResource",
        "kafka:TagResource",
        "kafka:UntagResource",
        "kendra:TagResource",
        "kendra:UntagResource",
        "kinesis:AddTagsToStream",
        "kinesis:RemoveTagsFromStream",
        "kinesisanalytics:TagResource",
        "kinesisanalytics:UntagResource",
        "kms:TagResource",
        "kms:UntagResource",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lex:TagResource",
        "lex:UntagResource",
        "license-manager:TagResource",
        "license-manager:UntagResource",
        "lightsail:TagResource",
        "lightsail:UntagResource",
        "logs:TagLogGroup",
        "logs:TagResource",
        "logs:UntagLogGroup",
        "logs:UntagResource",
        "lookoutequipment:TagResource",
        "lookoutequipment:UntagResource",
        "machinelearning:AddTags",
        "machinelearning:DeleteTags",
        "macie2:TagResource",
        "macie2:UntagResource",
```

```
        "managedblockchain:TagResource",
        "managedblockchain:UntagResource",
        "mediaconnect:TagResource",
        "mediaconnect:UntagResource",
        "mediaconvert:TagResource",
        "mediaconvert:UntagResource",
        "medialive:CreateTags",
        "medialive:DeleteTags",
        "mediapackage-vod:TagResource",
        "mediapackage-vod:UntagResource",
        "mediapackage:TagResource",
        "mediapackage:UntagResource",
        "mediatailor:TagResource",
        "mediatailor:UntagResource",
        "mobiletargeting:TagResource",
        "mobiletargeting:UntagResource",
        "mq:CreateTags",
        "mq:DeleteTags",
        "neptune-graph:TagResource",
        "neptune-graph:UntagResource",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "networkmanager:TagResource",
        "networkmanager:UntagResource",
        "opsworks-cm:TagResource",
        "opsworks-cm:UntagResource",
        "opsworks:TagResource",
        "opsworks:UntagResource",
        "organizations:TagResource",
        "organizations:UntagResource",
        "outposts:TagResource",
        "outposts:UntagResource",
        "qldb:TagResource",
        "qldb:UntagResource",
        "quicksight:TagResource",
        "quicksight:UntagResource",
        "ram:TagResource",
        "ram:UntagResource",
        "rds:AddTagsToResource",
        "rds:RemoveTagsFromResource",
        "redshift:CreateTags",
        "redshift:DeleteTags",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
```

```
        "resource-groups:Tag",
        "resource-groups:Untag",
        "robomaker:TagResource",
        "robomaker:UntagResource",
        "route53:ChangeTagsForResource",
        "route53domains:DeleteTagsForDomain",
        "route53domains:UpdateTagsForDomain",
        "route53resolver:TagResource",
        "route53resolver:UntagResource",
        "s3:GetBucketTagging",
        "s3:GetJobTagging",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionTagging",
        "s3:GetStorageLensConfigurationTagging",
        "s3:DeleteJobTagging",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:PutBucketTagging",
        "s3:PutJobTagging",
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging",
        "s3:PutStorageLensConfigurationTagging",
        "s3:DeleteStorageLensConfigurationTagging",
        "s3:TagResource",
        "s3:UntagResource",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "savingsplans:TagResource",
        "savingsplans:UntagResource",
        "schemas:TagResource",
        "schemas:UntagResource",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "securityhub:TagResource",
        "securityhub:UntagResource",
        "servicediscovery:TagResource",
        "servicediscovery:UntagResource",
        "servicequotas:TagResource",
        "servicequotas:UntagResource",
        "ses:TagResource",
        "ses:UntagResource",
        "sns:TagResource",
        "sns:UntagResource",
        "sqs:TagQueue",
```

```
        "sqs:UntagQueue",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "states:TagResource",
        "states:UntagResource",
        "storagegateway:AddTagsToResource",
        "storagegateway:RemoveTagsFromResource",
        "swf:TagResource",
        "swf:UntagResource",
        "synthetics:TagResource",
        "synthetics:UntagResource",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "transfer:TagResource",
        "transfer:UntagResource",
        "waf-regional:TagResource",
        "waf-regional:UntagResource",
        "waf:TagResource",
        "waf:UntagResource",
        "wafv2:TagResource",
        "wafv2:UntagResource",
        "worklink:TagResource",
        "worklink:UntagResource",
        "workmail:TagResource",
        "workmail:UntagResource",
        "workspaces:CreateTags",
        "workspaces:DeleteTags",
        "xray:TagResource",
        "xray:UntagResource",
        "kinesisvideo:TagResource",
        "kinesisvideo:UntagResource",
        "redshift-serverless:TagResource",
        "redshift-serverless:UntagResource",
        "route53-recovery-control-config:TagResource",
        "route53-recovery-control-config:UntagResource",
        "route53-recovery-readiness:TagResource",
        "route53-recovery-readiness:UntagResource",
        "ssm-contacts:TagResource",
        "ssm-contacts:UntagResource",
        "ssm-incidents:TagResource",
        "ssm-incidents:UntagResource",
        "vpc-lattice:TagResource",
        "vpc-lattice:UntagResource",
```

```
        "workspaces-web:TagResource",
        "workspaces-web:UntagResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSAAmazonEBSCSIDriverOperatorPolicy

Descrizione: consente all'operatore del driver OpenShift Amazon EBS Container Storage Interface (CSI) di installare e gestire il driver Amazon EBS CSI su un cluster Red Hat OpenShift Service on AWS (ROSA). Il driver Amazon EBS CSI consente ai cluster ROSA di gestire il ciclo di vita dei volumi Amazon EBS per volumi persistenti.

`ROSAAmazonEBSCSIDriverOperatorPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `ROSAAmazonEBSCSIDriverOperatorPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2023, 22:36 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVolumeFromSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "CreateSnapshotResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSACloudNetworkConfigOperatorPolicy

Descrizione: Consente all'operatore OpenShift Cloud Network Config Controller di fornire e gestire le risorse di rete per l'utilizzo da parte dell'overlay di rete del cluster Red Hat OpenShift Service on AWS (ROSA). Il OpenShift Cloud Network Operator si interfaccia con le AWS API per conto dei plugin di rete tramite. CustomResourceDefinitions L'operatore utilizza queste autorizzazioni di policy per gestire gli indirizzi IP privati per le istanze Amazon EC2 come parte del cluster ROSA.

`ROSACloudNetworkConfigOperatorPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `ROSACloudNetworkConfigOperatorPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 20 aprile 2023, 22:34 UTC
- Ora modificata: 20 aprile 2023, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyEIPs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSAControlPlaneOperatorPolicy

Descrizione: consente a Red Hat OpenShift Service on AWS (ROSA) di gestire le risorse del cluster ROSA Amazon EC2 e Amazon Route 53.

`ROSAControlPlaneOperatorPolicy`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ROSAControlPlaneOperatorPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica relativa al ruolo del servizio
- Ora di creazione: 24 aprile 2023, 23:02 UTC
- Ora modificata: 28 luglio 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Versione della politica

Versione della politica: v7 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "route53:ListHostedZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "ListResourceRecordSets",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointResourceTagCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
```

```
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "AddDeleteTagsRedHatManagedSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "red-hat-managed"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSAImageRegistryOperatorPolicy

Descrizione: consente all' OpenShift Image Registry Operator di effettuare il provisioning e la gestione di bucket e oggetti Amazon S3 per l'utilizzo da parte del registro di immagini interno al cluster Red Hat OpenShift Service on AWS (ROSA) per soddisfare i requisiti di storage ROSA. L' OpenShift Image Registry Operator installa e gestisce il registro interno di un cluster Red Hat. OpenShift

`ROSAImageRegistryOperatorPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ROSAImageRegistryOperatorPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 aprile 2023, 20:13 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
      ]
    },
    {
      "Sid" : "AllowSpecificObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
```

```
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSAIngressOperatorPolicy

Descrizione: Consente all'operatore OpenShift Ingress di fornire e gestire sistemi di bilanciamento del carico e configurazioni DNS (Domain Name System) per i cluster Red Hat OpenShift Service on AWS (ROSA). La policy consente l'accesso in lettura ai valori dei tag, che l'operatore filtra per le risorse Route 53 per scoprire le zone ospitate.

`ROSAIngressOperatorPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ROSAIngressOperatorPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2023, 22:37 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSAInstallerPolicy

Descrizione: Consente al programma di installazione di Red Hat OpenShift Service on AWS (ROSA) di gestire AWS le risorse che supportano l'installazione del cluster ROSA. Ciò include la gestione dei profili di istanza per i nodi di lavoro ROSA.

`ROSAInstallerPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ROSAInstallerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 6 giugno 2023, 21:00 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeCapacityReservations",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEC2",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
```

```
      ],
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "GetSecretValue",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ManageRecords",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.hypershift.local",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "Route53Manage",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RunInstancesRestrictedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRedHatOwnedAMIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstancesRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
```

```
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "CreateTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "ListPoliciesAttachedToRoles",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSAKarpenterControllerPolicy

Descrizione: fornisce le autorizzazioni al controller ROSA Karpenter per fornire e gestire dinamicamente le istanze EC2 per Red Hat OpenShift Service su cluster di piani di controllo ospitati AWS (ROSA). Ciò include la gestione del parco veicoli e del ciclo di vita delle istanze EC2, le richieste relative ai prezzi delle istanze, le operazioni KMS per la crittografia dei volumi EBS con chiavi gestite dal cliente e la gestione dei profili delle istanze IAM.

`ROSAKarpenterControllerPolicy`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `ROSAKarpenterControllerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica relativa al ruolo del servizio
- Ora di creazione: 27 luglio 2026, 16:42 UTC
- Ora modificata: 27 luglio 2026, 16:42 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKarpenterControllerPolicy`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PricingReadActions",
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DescribeKMSKeysForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CryptoOpsForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        }
      }
    },
    {
      "Sid" : "CreateGrantForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
```

```
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo"
          ],
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ]
    },
    {
      "Sid" : "CreateEC2ResourcesWithApprovedAMIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEC2ResourcesWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEC2ResourcesLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "CreateTagsOnResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate"
          ],
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageTagsOnManagedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "TerminateManagedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
```

```
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "PassInstanceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*-ROSA-Worker-Role",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
```

```
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ReadInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSAKMSProviderPolicy

Descrizione: consente al ROSA AWS Encryption Provider integrato di gestire le AWS chiavi KMS (Key Management Service) per supportare la crittografia dei dati etcd utilizzando una chiave AWS KMS fornita dal cliente. La politica consente la crittografia e la decrittografia dei dati utilizzando le chiavi KMS.

`ROSAKMSProviderPolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `ROSAKMSProviderPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 aprile 2023, 20:10 UTC
- Ora modificata: 27 aprile 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSAKubeControllerPolicy

Descrizione: consente al controller ROSA Kubernetes di gestire le risorse Amazon EC2, Elastic Load Balancing (ELB) e AWS Key Management Service (KMS) per un cluster ROSA.

`ROSAKubeControllerPolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `ROSAKubeControllerPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 aprile 2023, 20:09 UTC
- Ora modificata: 10 aprile 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeLoadBalancerPolicies"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "LoadBalanacerManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateTargetGroup",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagementResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
```

```
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateListeners",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true",
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "CreateSecurityGroupVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateLoadBalancer",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifySecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsSecurityGroups",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageTargetGroup",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSAManageSubscription

Descrizione: Questa policy fornisce le autorizzazioni necessarie per gestire la sottoscrizione Red Hat OpenShift Service on AWS (ROSA).

`ROSAManageSubscription`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ROSAManageSubscription` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 aprile 2022, 20:58 UTC
- Ora modificata: 04 agosto 2023, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws-marketplace:ProductId" : [
            "34850061-abaf-402d-92df-94325c9e947f",
            "bfdca560-2c78-4e64-8193-794c159e6d30"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSANodePoolManagementPolicy

Descrizione: consente a Red Hat OpenShift Service on AWS (ROSA) di gestire le istanze EC2 del cluster come nodi di lavoro, inclusa l'autorizzazione per configurare gruppi di sicurezza e contrassegnare istanze e volumi. Questa policy consente inoltre l'uso di istanze EC2 con crittografia del disco fornita dalle AWS chiavi Key Management Service (KMS).

`ROSANodePoolManagementPolicy`è una policy gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `ROSANodePoolManagementPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica relativa al ruolo del servizio

- Ora di creazione: 08 giugno 2023, 20:48 UTC
- Ora modificata: 29 luglio 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Versione della politica

Versione della politica: v9 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassWorkerRole",
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "NetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfacesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRequest",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
```

```
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ]
    },
    {
      "Sid" : "RunInstancesRedHatAMI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822"
          ]
        }
      }
    },
    {
      "Sid" : "NodePoolSQSActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestricted",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSASharedVPCEndpointPolicy

Descrizione: Consente al programma di installazione di Red Hat OpenShift Service on AWS (ROSA) di configurare endpoint e gruppi di sicurezza VPC. Destinato all'uso su un VPC condiviso.

`ROSASharedVPCEndpointPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ROSASharedVPCEndpointPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 agosto 2025, 17:19 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCEndpointPolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointResourceTagCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVPCEndpoingNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSASharedVPCRoute53Policy

Descrizione: Consente all'installatore di Red Hat OpenShift Service on AWS (ROSA) di configurare i record di Route53. Destinato all'uso su un VPC condiviso.

`ROSASharedVPCRoute53Policy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ROSASharedVPCRoute53Policy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 11 agosto 2025, 17:19 UTC

- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCRoute53Policy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local",
            "*.openshiftapps.com",
            "*.devshift.org",
```

```
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "ChangeTagsForResourceNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSASRESupportPolicy

Descrizione: Fornisce a ROSA Site Reliability Engineering (SRE) le autorizzazioni necessarie per osservare, diagnosticare e supportare inizialmente AWS le risorse associate a Red Hat OpenShift Service on AWS (ROSA) sui cluster, inclusa la possibilità di modificare lo stato del nodo del cluster ROSA.

`ROSASRESupportPolicy`è una policy gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `ROSASRESupportPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio

- Ora di creazione: 1 giugno 2023, 14:36 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "DecribeIAMRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeScheduledInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "VPCNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudtrail",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeLoadBalancers",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
```

```
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAddressesAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeAddressesAttribute",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*"
    },
    {
      "Sid" : "DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeSpotFleetInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSpotFleetInstances",
      "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumeAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumeAttribute",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageInstanceLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ROSAWorkerInstancePolicy

Descrizione: consente ai nodi di lavoro Red Hat OpenShift Service on AWS (ROSA) del tuo account l'accesso in sola lettura alle istanze Amazon EC2 Regioni AWS e per la gestione del ciclo di vita dei nodi di calcolo.

`ROSAWorkerInstancePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `ROSAWorkerInstancePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 aprile 2023, 22:35 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2DescribeInstancesRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRGetAuthorizationToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRReadOnlyAccessRedHatManaged",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

Route53RecoveryReadinessServiceRolePolicy

Descrizione: policy Service Linked Role per la preparazione al ripristino della Route 53

`Route53RecoveryReadinessServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 15 luglio 2021, 16:06 UTC
- Ora modificata: 14 febbraio 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicequotas.amazonaws.com/
AWSServiceRoleForServiceQuotas",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction"
```

```
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHealthCheck",
        "route53:GetHealthCheckStatus"
      ],
      "Resource" : "arn:aws:route53:::healthcheck/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:RequestServiceQuotaIncrease"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic"
```

```
      ],
      "Resource" : "arn:aws:sns:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : "arn:aws:sqs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "dynamodb:DescribeLimits",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
```

```
        "elasticloadbalancing:DescribeTargetHealth",
        "kafka:DescribeCluster",
        "kafka:DescribeConfigurationRevision",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "rds:DescribeAccountAttributes",
        "route53:GetHostedZone",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "sns:GetEndpointAttributes",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

Route53ResolverServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Route53 Resolver

`Route53ResolverServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 12 agosto 2020, 17:47 UTC

- Ora modificata: 12 agosto 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

RTBFabricServiceRolePolicy

Descrizione: un ruolo collegato ai servizi necessario per AWS RTBFabric creare e gestire le risorse dell'interfaccia di rete e fornire metriche.

`RTBFabricServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 16 ottobre 2025, 16:49 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/RTBFabricServiceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "RTBFabricRoleCreateTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfacePermissionActions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleTaggingActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RTBFabricRolePutMetricDataActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/RTBFabric"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

S3StorageLensServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da S3 Storage Lens

`S3StorageLensServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 18 novembre 2020, 18:15 UTC
- Ora modificata: 18 novembre 2020, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
```

```
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioAdminIAMConsolePolicy

Descrizione: fornisce i privilegi di configurazione amministrativa e individuale iniziali per Amazon SageMaker Unified Studio tramite l'SDK Console di gestione AWS and. Consente il lancio di Unified Studio Portal. SageMaker

`SageMakerStudioAdminIAMConsolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioAdminIAMConsolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2025, 22:49 UTC
- Ora modificata: 27 marzo 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMConsolePolicy`

Versione della politica

Versione della politica: v8 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*"
      ]
    },
    {
      "Sid" : "DescribeEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSubnetInTaggedVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateTaggedSecurityGroupInVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpointInTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateInternetGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway"
      ],
      "Resource" : "arn:aws:ec2:*:*:internet-gateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedNatGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:natgateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNatGatewayInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllocateAddress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AttachInternetGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "Ec2TaggingOperations",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSubnet",
            "CreateSecurityGroup",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateRouteTable",
            "CreateVpcEndpoint"
          ],
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "Ec2TagEIP",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCFNStackCreation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:CreateStack",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteTaggedVpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:DeleteSubnet",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteInternetGateway",
        "ec2:DetachInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteRouteTable",
        "ec2:DeleteRoute",
        "ec2:ReleaseAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "DeleteTagsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "S3ReadCFNTemplate",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "DataZoneKMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "GlueCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DeleteApplication"
```

```
      ],
      "Resource" : [
        "arn:aws:sso::*:application/*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "datazone.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "SSOKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "false"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioAdminIAMDefaultExecutionPolicy

Descrizione: politica di esecuzione amministrativa per l'utilizzo dei ruoli IAM con SageMaker Unified Studio. Consente agli amministratori di effettuare il provisioning, gestire e accedere alle risorse del tuo account (escluso l'accesso alle risorse di dati) per l' IAM-based utilizzo di Unified Studio. SageMaker

`SageMakerStudioAdminIAMDefaultExecutionPolicy`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioAdminIAMDefaultExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2025, 17:19 UTC
- Ora modificata: 14 luglio 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMDefaultExecutionPolicy`

Versione della politica

Versione della politica: v24 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
```

```
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-unified-studio-mcp:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
```

```
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "SageMakerSpacesDomainId"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
```

```
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
```

```
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datazone.amazonaws.com",
            "bedrock.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "events.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Q",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
```

```
      ]
    },
    {
      "Sid" : "ManageSageMakerSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:Batch*",
        "sagemaker:DeleteTags",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:*MlflowApp*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
```

```
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*",
        "sagemaker:*Feature*",
        "sagemaker:*Record"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucketPolicy",
        "s3:Get*",
        "s3:Put*",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*",
        "arn:aws:cloudformation:*:*:transform/*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LFManage",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
```

```
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:*DataCellsFilter"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:connection/*"
      ]
    },
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
```

```
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:*Resource",
        "glue:UseGlueStudio",
        "glue:*Job*",
        "glue:TestConnection",
        "glue:*DataQuality*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
```

```
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowMWAA",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageScheduler",
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
```

```
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
```

```
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
```

```
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
```

```
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "EMR",
      "Effect" : "Allow",
```

```
      "Action" : [
        "emr-serverless:Get*",
        "emr-serverless:List*",
        "emr-serverless:Start*",
        "emr-serverless:Access*",
        "emr-serverless:Terminate*",
        "emr-serverless:*Resource",
        "emr-containers:*ManagedEndpoint*",
        "emr-containers:*SecurityConfiguration*",
        "emr-containers:*VirtualCluster*",
        "emr-containers:*Resource",
        "elasticmapreduce:*PersistentAppUI*",
        "elasticmapreduce:Start*",
        "elasticmapreduce:Get*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:Terminate*",
        "elasticmapreduce:*Tag*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:UpdateApplication",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "SSOReadOnlyPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sso:ListInstances",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IdentityStoreKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:Get*",
        "ram:List*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreateResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RAMResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RAMAssociateResourceSharePermission",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
```

```
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "CanvasGeneralPermissions",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:*",
        "textract:*",
        "rekognition:*",
        "sagemaker-data-science-assistant:*",
        "rds:DescribeDBInstances",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalingActivities",
        "quicksight:ListNamespaces",
        "events:PutRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:TagResource",
        "events:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CanvasRedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioAdminIAMPermissiveExecutionPolicy

Descrizione: politica di esecuzione amministrativa per l'utilizzo dei ruoli IAM con SageMaker Unified Studio. Consente agli amministratori di fornire, gestire e accedere alle risorse nell'account locale (incluso un ampio accesso a tutte le API nei servizi di dati come S3, Glue, CloudWatch Logs e altri) per IAM-based l'utilizzo di Unified Studio. SageMaker

`SageMakerStudioAdminIAMPermissiveExecutionPolicy`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioAdminIAMPermissiveExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2025, 17:19 UTC
- Ora modificata: 14 luglio 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMPermissiveExecutionPolicy`

Versione della politica

Versione della politica: v21 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*",
        "s3tables:*",
        "comprehend:*",
        "textract:*",
        "rekognition:*",
        "sagemaker-data-science-assistant:*",
        "rds:*",
        "quicksight:*",
        "events:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
        "datazone:*",
        "elasticmapreduce:*",
        "emr-containers:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
```

```
        "emr-serverless:*",
        "airflow-serverless:*",
        "airflow:*",
        "application-autoscaling:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*",
        "arn:aws:cloudformation:*:*:transform/*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
```

```
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
```

```
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
```

```
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "SageMakerSpacesDomainId"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "datazone.amazonaws.com",
```

```
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:*DataCellsFilter"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
```

```
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnections",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
```

```
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
```

```
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSG",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "SSOApplicationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
```

```
        "sso:PutApplicationGrant",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:UpdateApplication",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "SSOReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IdentityStoreKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreateResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RAMResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RAMAssociateResourceSharePermission",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioAdminProjectUserRolePolicy

Descrizione: questa policy IAM garantisce a un ruolo IAM l'accesso completo a AWS Glue Data Catalog (metadati) e Amazon S3 (dati effettivi) per le operazioni di data lake, con accesso limitato per account e tag di ruolo.

`SageMakerStudioAdminProjectUserRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioAdminProjectUserRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 luglio 2025, 20:52 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
```

```
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioBedrockAgentServiceRolePolicy

Descrizione: consente agli agenti Amazon Bedrock di accedere ai modelli Amazon Bedrock e ad altre risorse collegate a un agente in SageMaker Studio.

`SageMakerStudioBedrockAgentServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioBedrockAgentServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 13 febbraio 2025, 23:37 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockAgentServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "BedrockApplyGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrievePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "S3GetObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectAttributes"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioBedrockChatAgentUserRolePolicy

Descrizione: fornisce l'accesso alla configurazione di un'app agente di chat Amazon Bedrock e all'agente Amazon Bedrock in SageMaker Studio.

`SageMakerStudioBedrockChatAgentUserRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioBedrockChatAgentUserRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 13 febbraio 2025, 23:52 UTC

- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockChatAgentUserRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockGetAgentAliasPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetAgentAlias",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGetAndListAgentMetadataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions"
      ],
      "Resource" : "arn:aws:bedrock:*:*:agent/${aws:PrincipalTag/AgentId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3ListAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/AppDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
```

```
      }
    },
    {
      "Sid" : "S3GetAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AppDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3ListDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/DataSourcePath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
```

```
      "Sid" : "S3GetDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/DataSourcePath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/${aws:PrincipalTag/AgentId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
```

```
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioBedrockEvaluationJobServiceRolePolicy

Descrizione: consente ad Amazon Bedrock di accedere a modelli e set di dati Amazon Bedrock per lavori di valutazione in Studio. SageMaker

`SageMakerStudioBedrockEvaluationJobServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioBedrockEvaluationJobServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 febbraio 2025, 00:37 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockEvaluationJobServiceRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockEvaluationInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelInvocationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:GetProvisionedModelThroughput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetBucketLocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketLocation",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        }
```

```
      }
    },
    {
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "S3EvaluationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/${aws:PrincipalTag/
AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
```

```
      }
    },
    {
      "Sid" : "KmsDescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioBedrockFlowServiceRolePolicy

Descrizione: consente ad Amazon Bedrock Flows di accedere ai modelli Amazon Bedrock e ad altre risorse collegate a un flusso in SageMaker Studio.

`SageMakerStudioBedrockFlowServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioBedrockFlowServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 febbraio 2025, 00:07 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFlowServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowLambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockApplicationInferenceProfileAccessInProjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockInvokeModelAccessWithInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioBedrockFunctionExecutionRolePolicy

Descrizione: consente a AWS Lambda di accedere alla configurazione di un componente della funzione Amazon Bedrock in Studio. SageMaker

`SageMakerStudioBedrockFunctionExecutionRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioBedrockFunctionExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 25 febbraio 2025, 03:52 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFunctionExecutionRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
```

```
        }
      }
    },
    {
      "Sid" : "KMSSameAccountBedrockViaSecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:amazon-bedrock*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

Descrizione: fornisce l'accesso per configurare gli archivi vettoriali e le knowledge base Amazon Bedrock in SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 25 febbraio 2025, 03:37 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetIngestionJob",
```

```
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob"
      ],
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

Descrizione: consente ad Amazon Bedrock Knowledge Bases di accedere ai modelli e alle origini dati di Amazon Bedrock in SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 25 febbraio 2025, 02:52 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
```

```
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
```

```
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "VectorStoresKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "VectorStoresKmsDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NeptuneGraphDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:GetGraph",
        "neptune-graph:DeleteDataViaQuery",
        "neptune-graph:WriteDataViaQuery",
        "neptune-graph:ReadDataViaQuery"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3VectorsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:GetVectorBucket",
        "s3vectors:GetIndex",
```

```
        "s3vectors:PutVectors",
        "s3vectors:GetVectors",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "s3vectors:DeleteVectors"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-${aws:PrincipalTag/
AmazonDataZoneProject}*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:knowledge-base/*"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    },
    {
      "Sid" : "SqlWorkbenchAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetSqlRecommendations",
        "sqlworkbench:PutSqlGenerationContext",
        "sqlworkbench:GetSqlGenerationContext",
        "sqlworkbench:DeleteSqlGenerationContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockGenerateQueryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioBedrockPromptUserRolePolicy

Descrizione: fornisce l'accesso a un prompt di Amazon Bedrock e alla sua configurazione in SageMaker Studio.

`SageMakerStudioBedrockPromptUserRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioBedrockPromptUserRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 14 febbraio 2025, 00:22 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockPromptUserRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/${aws:PrincipalTag/PromptId}:
${aws:PrincipalTag/PromptVersion}",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3ListPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/PromptDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/PromptDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/${aws:PrincipalTag/PromptId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
```

```
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioDomainExecutionRolePolicy

Descrizione: questa policy viene utilizzata da Amazon SageMaker Studio per catalogare, scoprire, governare, condividere e analizzare i dati nel dominio Amazon SageMaker Studio.

`SageMakerStudioDomainExecutionRolePolicy`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioDomainExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica relativa al ruolo del servizio
- Ora di creazione: 20 novembre 2024, 21:56 UTC
- Ora modificata: 3 agosto 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainExecutionRolePolicy`

Versione della politica

Versione della politica: v22 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:AssociateGovernedTerms",
        "datazone:BatchGetAttributesMetadata",
        "datazone:BatchPutAttributesMetadata",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateConnection",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteConnection",
        "datazone:DeleteDataProduct",
```

```
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:DisassociateGovernedTerms",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetConnection",
        "datazone:GetCurrentEffectivePolicy",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDesignation",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
```

```
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUpdateEligibility",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListConnections",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDesignations",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:QueryGraph",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
```

```
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "q:GetIdentityMetadata",
        "glue:StartCompletion",
```

```
        "glue:GetCompletion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q/${aws:PrincipalTag/datazone-
domainId}*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/${aws:PrincipalTag/datazone-
domainId}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
```

```
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ListCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "UseCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ProjectProfilePermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetProjectProfile",
        "datazone:ListProjectProfiles"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
    },
    {
      "Sid" : "AccountPoolPermissionsStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetAccountPool",
        "datazone:ListAccountPools",
        "datazone:ListAccountsInAccountPool"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioDomainServiceRolePolicy

Descrizione: ruolo di servizio per le azioni a livello di dominio nel portale eseguite da Amazon SageMaker Studio.

`SageMakerStudioDomainServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioDomainServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 novembre 2024, 21:56 UTC
- Ora modificata: 20 novembre 2024, 21:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles/*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com",
          "kms:EncryptionContext:PARAMETER_ARN" : "arn:aws:ssm:*:*:parameter/amazon/
datazone/profiles*"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioEMRContainersSystemNamespaceRolePolicy

Descrizione: Amazon SageMaker Studio crea ruoli IAM per gli utenti del progetto per eseguire analisi dei dati, intelligenza artificiale e azioni di apprendimento automatico e utilizza questa politica durante la creazione di questi ruoli per definire le autorizzazioni relative all'EMR.

`SageMakerStudioEMRContainersSystemNamespaceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioEMRContainersSystemNamespaceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 23 ottobre 2025, 18:34 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRContainersSystemNamespaceRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AssumeProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "TagSessionProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/LakeFormationAuthorizedCaller" : "EMR on EKS Engine",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SetContextProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioEMRInstanceRolePolicy

Descrizione: Amazon SageMaker Studio crea ruoli IAM per gli utenti del progetto per eseguire analisi dei dati, intelligenza artificiale e azioni di apprendimento automatico e utilizza questa politica durante la creazione di questi ruoli per definire le autorizzazioni relative all'EMR.

`SageMakerStudioEMRInstanceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioEMRInstanceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 27 febbraio 2025, 00:22 UTC
- Ora modificata: 01 giugno 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRInstanceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCertificateLocationS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
```

```
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessPatchingRPMsS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:::awssmuscompute-blueprint-bucket-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*",
        "arn:aws:s3:*:*:accesspoint/env-partner-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : [
            "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint",
            "arn:aws:s3:*:*:accesspoint/env-partner-blueprint-accesspoint"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessBootstrapActionScriptS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/bootstrap-script/*",
```

```
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRClusterLogUploadS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRRuntimeRoleAssumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
          "iam:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioEMRServiceRolePolicy

Descrizione: Amazon SageMaker Studio crea ruoli IAM per gli utenti del progetto per eseguire analisi dei dati, intelligenza artificiale e azioni di apprendimento automatico e utilizza questa politica durante la creazione di questi ruoli per definire le autorizzazioni relative all'EMR.

`SageMakerStudioEMRServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioEMRServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 31 gennaio 2025, 19:52 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy`

Versione della politica

Versione della politica: v9 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassRoleToEMREC2InstanceRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_
${aws:PrincipalTag/AmazonDataZoneProject}_${aws:PrincipalTag/
AmazonDataZoneEnvironment}",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneEnvironment" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateInNetworkForSharedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeKeyForLogPusherCMK",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioFullAccess

Descrizione: questa policy fornisce l'accesso completo ad Amazon SageMaker Unified Studio tramite la console di SageMaker gestione Amazon.

`SageMakerStudioFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 28 novembre 2024, 00:06 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioFullAccess`

Versione della politica

Versione della politica: v15 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "iam:ListPolicies",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
```

```
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
        "aoss:ListSecurityPolicies",
        "quicksight:DescribeAccountSubscription",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "ReadManagedBlueprintTemplatesStatement",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/env-blueprint-
accesspoint"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PutObjectStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
```

```
    {
      "Sid" : "ConnectionStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
```

```
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
```

```
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "ModelAccessUseCaseStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetUseCaseForModelAccess",
```

```
        "bedrock:PutUseCaseForModelAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioProjectProvisioningRolePolicy

Descrizione: Amazon SageMaker Studio utilizza questa politica per fornire e gestire le risorse nel tuo account.

`SageMakerStudioProjectProvisioningRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioProjectProvisioningRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 novembre 2024, 21:58 UTC
- Ora modificata: 04 giugno 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioProjectProvisioningRolePolicy`

Versione della politica

Versione della politica: v81 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnMng",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:DescribeStackEvents",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnDelete",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Discovery",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "bedrock:ListEvaluationJobs",
        "cloudformation:ValidateTemplate",
        "codecommit:ListRepositories",
        "eks:DescribeCluster",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "glue:DescribeConnectionType",
```

```
        "glue:ListConnectionTypes",
        "glue:*GlueIdentityCenterConfiguration",
        "iam:ListPolicies",
        "logs:DescribeLogGroups",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeDataSharesForConsumer",
        "redshift:GetResourcePolicy",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LFMng",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:DescribeResource",
        "lakeformation:*LakeFormationIdentityCenterConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DzTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
```

```
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DzCfTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::amazon-sagemaker-cf-templates*/*"
    },
    {
      "Sid" : "CcCreate",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateRepository",
        "codecommit:TagResource"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcDelete",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:DeleteRepository",
        "codecommit:UntagResource",
        "codecommit:UpdateRepositoryEncryptionKey",
        "codecommit:PutRepositoryTriggers"
      ],
```

```
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetBranch",
        "codecommit:CreateCommit",
        "codecommit:GetRepository",
        "codecommit:GetFile"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetIamRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ]
    },
    {
      "Sid" : "IAMMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrockExecution*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/AmazonBedrockConsumptionRole*",
        "arn:aws:iam::*:role/AmazonBedrockEvaluation*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
```

```
    },
    {
      "Sid" : "IamDzMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "RoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRContainersSystemNamespaceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRInstanceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2",
            "arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicyForSessions",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole",
            "arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamMngAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioAdminIAMDefaultExecutionPolicy"
          ]
        },
```

```
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneAdminProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamMngBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockAgentServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockChatAgentUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFlowServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFunctionExecutionRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockPromptUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockEvaluationJobServiceRolePolicy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamTag",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/datazone_redshift_serverless_admin_role_*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "BootstrappedServices",
            "AmazonBedrockManaged",
            "RedshiftDb*",
            "EnableAmazonBedrockPermissions",
            "EnableAmazonBedrockIDEPermissions",
            "EnableGlueWorkloadsPermissions",
            "EnableSageMakerMLWorkloadsPermissions",
            "DomainBucketName",
            "KmsKeyId",
            "DomainKmsKeyId",
            "DefaultGlueCatalogKmsKeyId",
            "LogGroupName",
            "RoleName",
            "vpcArn",
            "VpcId",
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole",
            "SageMakerSpacesDomainId"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AdminProjectTagRoleMng",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneScopeName",
            "BootstrappedServices",
            "AmazonDataZoneAdminProject"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamTagBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "DomainBucketName",
            "KmsKeyId",
            "AgentId",
            "AgentAliasId",
            "AppDefinitionPath",
            "DataSourcePath",
            "PromptId",
            "PromptVersion",
            "PromptDefinitionPath",
            "OpenSearchServerlessCollectionId"
```

```
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamTagRS",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "RedshiftDb*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "IamTagEMR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*",
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*",
        "arn:aws:iam::*:role/datazone_emr_containers_system_namespace_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "DataZone*",
            "for-use-with-amazon-emr-managed-policies",
```

```
            "DomainBucketName",
            "KmsKeyId",
            "VpcId"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "IamUntag",
      "Effect" : "Allow",
      "Action" : "iam:UntagRole",
      "Resource" : "arn:aws:iam::*:role/datazone_usr_role_*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "EnableAmazonBedrockIDEPermissions"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "DzMngRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateAssumeRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_emr_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamAttach",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "IamDetach",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ]
    },
    {
      "Sid" : "DzMngPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:CreatePolicyVersion",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:iam::*:policy/connector-manage-access-policy*",
        "arn:aws:iam::*:policy/SageMakerStudioQueryExecutionRolePolicy"
      ]
    },
    {
      "Sid" : "InstanceProfile",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ],
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow.amazonaws.com",
            "athena.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForDZ",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForGlue",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
```

```
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmr",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticmapreduce.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmrIP",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBR",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRoleToLambda",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AossSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog/*",
        "arn:aws:glue:*:*:database/s3tablescatalog/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnGlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "GlueDbDelete",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnTag",
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnMng",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnections",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaConnection",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateDataCatalog"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GetConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "ConnectionTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "federated_athena*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "CreateConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngCatalogConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetDataCatalogEncSett",
      "Effect" : "Allow",
      "Action" : "glue:GetDataCatalogEncryptionSettings",
      "Resource" : "arn:aws:glue:*:*:catalog",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Repo",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:GetCloudFormationTemplate",
        "serverlessrepo:CreateCloudFormationTemplate"
      ],
```

```
      "Resource" : [
        "arn:aws:serverlessrepo:*:*:applications/Athena*"
      ]
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/athena-federation-repository*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CfnChangeSet",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:transform/*"
      ]
    },
    {
      "Sid" : "LambdaMng",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaGet",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "athena.amazonaws.com",
            "cloudformation.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
```

```
            "aws:cloudformation:*",
            "federated_athena*",
            "lambda:createdBy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaS3Get",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaLast" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "Null" : {
          "s3:prefix" : "true"
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3Create",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "Cfn",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/athenafederatedcatalog*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/federated_athena_datacatalog" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaDC",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteDataCatalog",
        "athena:GetDataCatalog",
```

```
        "athena:UpdateDataCatalog"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ]
    },
    {
      "Sid" : "S3tPassConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/aws:s3tables"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true"
        }
      }
    },
    {
      "Sid" : "GlueCatalogCreate",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueCatalogMgmt",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RSMng",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteNamespace",
        "redshift-serverless:DeleteWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshotcopyconfiguration/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataShare",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift:AssociateDataShareConsumer",
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "redshift-serverless.amazonaws.com",
            "glue.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SGMng",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGRevoke",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagEc2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
```

```
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2Mng",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged"
```

```
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LGRetention",
      "Effect" : "Allow",
      "Action" : "logs:PutRetentionPolicy",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:UntagResource",
        "logs:DeleteRetentionPolicy",
        "logs:GetDataProtectionPolicy",
        "logs:PutDataProtectionPolicy",
        "logs:DeleteDataProtectionPolicy",
        "logs:AssociateKmsKey",
        "logs:DisassociateKmsKey",
        "logs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AthenaMng",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AthenaWGDelete",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "athena:UpdateWorkGroup",
        "athena:UntagResource",
        "athena:GetWorkGroup"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftCreate",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagRSS",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false"
        }
      }
    },
    {
      "Sid" : "SecretProject",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SecretAll",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "TagSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "CreatedBy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SecretKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
```

```
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SsoKms",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IdStoreKms",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
```

```
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/emr-containers.amazonaws.com/
AWSServiceRoleForAmazonEMRContainers",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "RssMng",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:UntagResource",
        "redshift-serverless:UpdateNamespace",
        "redshift-serverless:UpdateWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:redshift-serverless:arn" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "redshift-serverless.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BRSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
```

```
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagRsSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "Redshift",
            "aws:secretsmanager:*",
            "aws:redshift-serverless:*",
            "AmazonDataZone*",
            "datazone.rs.workgroup"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
```

```
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagSMDForUpdate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain",
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateDomain",
        "sagemaker:DeleteDomain"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:domain/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SMAppDelete",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteApp",
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteSpace",
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteUserProfile",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteUserProfile",
```

```
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSCreate",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:CreateApplication",
        "emr-serverless:TagResource"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSMng",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:DeleteApplication",
        "emr-serverless:GetApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:UpdateApplication"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Eni",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Subnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MLFlowCreate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowTrackingServer",
        "sagemaker:AddTags"
```

```
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MLFlowDescribe",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeMlflowTrackingServer",
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
    },
    {
      "Sid" : "MLFlowDelete",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteMlflowTrackingServer"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MLFlowServerlessCreate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "MLFlowServerlessDescribeDelete",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteMlflowApp",
        "sagemaker:DescribeMlflowApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AossMng",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:UpdateAccessPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*",
          "aoss:index" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "MngAossPolicies",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetAoss",
      "Effect" : "Allow",
      "Action" : "aoss:BatchGetCollection",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AossCollections",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection",
        "aoss:UpdateCollection",
        "aoss:DeleteCollection",
        "aoss:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:UpdateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:GetGraph"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3VectorsMng",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:CreateVectorBucket",
        "s3vectors:DeleteVectorBucket",
        "s3vectors:ListVectorBuckets",
        "s3vectors:GetVectorBucket",
        "s3vectors:CreateIndex",
        "s3vectors:DeleteIndex",
        "s3vectors:ListIndexes",
        "s3vectors:GetIndex"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:TagResource"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrock*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "GetS3GenAI",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/dzd*/*/genAI/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetBR",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetGuardrail",
        "bedrock:GetPrompt",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BRMng",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateAgent",
        "bedrock:UpdateAgent",
        "bedrock:PrepareAgent",
        "bedrock:DeleteAgent",
```

```
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentAlias",
        "bedrock:CreateAgentAlias",
        "bedrock:UpdateAgentAlias",
        "bedrock:DeleteAgentAlias",
        "bedrock:ListAgentActionGroups",
        "bedrock:GetAgentActionGroup",
        "bedrock:CreateAgentActionGroup",
        "bedrock:UpdateAgentActionGroup",
        "bedrock:DeleteAgentActionGroup",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:AssociateAgentKnowledgeBase",
        "bedrock:DisassociateAgentKnowledgeBase",
        "bedrock:UpdateAgentKnowledgeBase",
        "bedrock:CreateKnowledgeBase",
        "bedrock:UpdateKnowledgeBase",
        "bedrock:DeleteKnowledgeBase",
        "bedrock:ListDataSources",
        "bedrock:GetDataSource",
        "bedrock:CreateDataSource",
        "bedrock:UpdateDataSource",
        "bedrock:DeleteDataSource",
        "bedrock:ListIngestionJobs",
        "bedrock:GetIngestionJob",
        "bedrock:StartIngestionJob",
        "bedrock:StopIngestionJob",
        "bedrock:CreateGuardrail",
        "bedrock:UpdateGuardrail",
        "bedrock:DeleteGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreatePrompt",
        "bedrock:UpdatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:CreateFlow",
        "bedrock:UpdateFlow",
        "bedrock:PrepareFlow",
        "bedrock:DeleteFlow",
        "bedrock:ListFlowAliases",
        "bedrock:GetFlowAlias",
        "bedrock:CreateFlowAlias",
        "bedrock:UpdateFlowAlias",
        "bedrock:DeleteFlowAlias",
```

```
        "bedrock:ListFlowVersions",
        "bedrock:GetFlowVersion",
        "bedrock:CreateFlowVersion",
        "bedrock:DeleteFlowVersion",
        "bedrock:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagBR",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : [
        "arn:aws:bedrock:*:*:agent-alias/*/TSTALIASID",
        "arn:aws:bedrock:*:*:flow/*/alias/TSTALIASID"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngBRJobs",
      "Effect" : "Allow",
      "Action" : "bedrock:BatchDeleteEvaluationJob",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "BRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:GetPolicy",
        "lambda:AddPermission",
        "lambda:TagResource"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngBRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "EMRClusterMng",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AirflowEnv",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:DeleteEnvironment",
        "airflow:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AirflowS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpcCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ENICreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "KmsCreate",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "airflow.*.amazonaws.com",
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KmsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QueryRoleMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "QueryRoleCreate",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "QueryRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioQueryExecutionRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "TagQueryRole",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
    {
      "Sid" : "ListQueryPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
```

```
    },
    {
      "Sid" : "EMRCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrRoleCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone_emr_*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrInstanceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
    {
      "Sid" : "Scheduler",
```

```
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListTagsForResource",
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ScheduleGroup",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteScheduleGroup",
        "scheduler:UntagResource"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:CreateScheduleGroup",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "TagSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:TagResource",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteSchedule",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/SageMakerUnifiedStudio-*-*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngQSFolder",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
```

```
        "quicksight:CreateFolder",
        "quicksight:CreateFolderMembership",
        "quicksight:CreateVPCConnection",
        "quicksight:DeleteDataSource",
        "quicksight:DeleteFolder",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListFolderMembers",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:UpdateFolder",
        "quicksight:UpdateFolderPermissions",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuickSightResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeGroup",
        "quicksight:DescribeGroupMembership",
        "quicksight:DescribeUser",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDashboardPermissions"
```

```
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagQS",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:TagResource"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRoleForQS",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQuickSightVPC",
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "quicksight.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "PutRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.quicksight",
            "aws.codecommit"
          ]
        },
        "Null" : {
          "events:detail-type" : "false",
          "events:source" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "datazone.amazonaws.com",
          "events:detail-type" : [
            "AWS Service Event via CloudTrail",
            "CodeCommit Repository State Change"
          ]
        }
      }
    },
    {
      "Sid" : "MngEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "datazone.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "RssAdmin",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGPerm",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstance",
        "s3:CreateAccessGrantsInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ResourceTagsUnTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:UntagResource",
        "neptune-graph:UntagResource",
        "quicksight:UntagResource",
        "glue:UntagResource",
        "airflow:UntagResource",
        "secretsmanager:UntagResource",
        "lambda:UntagResource",
        "emr-serverless:UntagResource",
```

```
        "elasticmapreduce:RemoveTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSOMng",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationSessionConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "elasticmapreduce.amazonaws.com",
            "emr-containers.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "ops.emr-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EmrContainersMng",
      "Effect" : "Allow",
```

```
      "Action" : [
        "emr-containers:CreateManagedEndpoint",
        "emr-containers:CreateSecurityConfiguration",
        "emr-containers:CreateVirtualCluster",
        "emr-containers:DeleteManagedEndpoint",
        "emr-containers:DeleteSecurityConfiguration",
        "emr-containers:DeleteVirtualCluster",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngViaEmrContainers",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "eks:AssociateAccessPolicy",
        "eks:CreateAccessEntry",
        "eks:DisassociateAccessPolicy",
        "eks:DeleteAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioProjectRoleMachineLearningPolicy

Descrizione: Amazon SageMaker Studio crea ruoli IAM per consentire agli utenti del progetto di eseguire analisi dei dati, intelligenza artificiale e azioni di apprendimento automatico e utilizza questa politica durante la creazione di questi ruoli per definire le autorizzazioni relative a SageMaker.

`SageMakerStudioProjectRoleMachineLearningPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioProjectRoleMachineLearningPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2024, 21:55 UTC
- Ora modificata: 09 luglio 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy`

Versione della politica

Versione della politica: v41 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowManageSageMakerEniOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        },
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "sagemaker.amazonaws.com",
            "airflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerTrainingEniOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpointOnVpcId",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}",
      "Condition" : {
        "StringEquals" : {
          "ec2:VpcID" : "${aws:PrincipalTag/VpcId}"
        },
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDescribeVPCResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSageMakerLogAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
```

```
      "Sid" : "SageMakerMlflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerMlflowServerlessPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowApp",
        "sagemaker:CreatePresignedMlflowAppUrl",
        "sagemaker:DeleteMlflowApp",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:UpdateMlflowApp",
        "sagemaker:CallMlflowAppApi"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerBYOFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SageMakerBYOIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeImageVersion",
        "sagemaker:ListImageVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeImageActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeImage"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:image/*"
    },
    {
      "Sid" : "SageMakerPipelinesSTSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerLogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "SageMakerCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
```

```
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:CreatePipeline",
        "sagemaker:CreateInferenceRecommendationsJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerInferencePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StopTrainingJob",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
```

```
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerUpdateInferenceComponentRuntimeConfigAutoscalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateInferenceComponentRuntimeConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerDescribeUpdateDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:UpdatePipeline",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DeletePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:StartPipelineExecution",
```

```
        "sagemaker:StopPipelineExecution",
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateContext",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAction",
        "sagemaker:AddAssociation",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteArtifact"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "SageMakerModelRegistryLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:QueryLineage",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:GetSearchSuggestions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListHubs",
        "sagemaker:ListPipelines",
        "sagemaker:ListContexts",
        "sagemaker:ListMlflowApps",
        "sagemaker:ListFeatureGroups",
        "scheduler:ListSchedules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerSearchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Search"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "sagemaker:SearchVisibilityCondition/Tags.AmazonDataZoneProject/
EqualsIfExists" : "${aws:PrincipalTag/AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerListPermissionsTagRestricted",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListHubContents",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerPublicHubReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHubContent",
        "sagemaker:ListHubContents"
      ],
```

```
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub",
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "SageMakerECRGetAuthorizationTokenPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
```

```
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerMLFlowModelRegistrationPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackageGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:model-package-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForTaggedUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppListActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListSpaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeDomainActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeJupyterLabAppActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
```

```
      ]
    },
    {
      "Sid" : "SageMakerStudioAppDescribeUserProfileActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeTaggedUserProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SMStudioAppDescribeSpaceActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeSpace"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model"
          ]
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingTaggedOwnerUserProfile",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
```

```
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
```

```
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "PublishSagemakerMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "/aws/sagemaker/*"
```

```
        }
      }
    },
    {
      "Sid" : "ManageSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MutateSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
    },
    {
      "Sid" : "SageMakerJumpstartS3Access",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-*/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCrossAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:ListModelPackages",
        "sagemaker:CreateModel"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerListTagsRestrictionOnSharedResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerFeatureStorePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*Feature*",
        "sagemaker:*Record"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissionsWithserviceNamespace",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "sagemaker.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3AGObjectRead",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGObjectWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGBucketLevelReadPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3AGLocationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrantsLocation",
        "s3:DeleteAccessGrantsLocation",
        "s3:GetAccessGrantsLocation"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:*:*:access-grants/default/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:accessGrantsLocationScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/"
        }
      }
    },
    {
      "Sid" : "S3AGPermissionManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrant",
        "s3:DeleteAccessGrant"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:accessGrantScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "s3:AccessGrants"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutAccessGrantsInstanceResourcePolicy"
      ],
      "Resource" : "arn:aws:s3:*:*:access-grants/default",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:TagResource",
        "s3:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsumerS3AGPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MLAccountDiscovery",
```

```
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:ListWorkflow*",
        "airflow-serverless:ListTask*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowServerlessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:GetTaskInstance",
        "airflow-serverless:GetWorkflow",
        "airflow-serverless:GetWorkflowRun",
        "airflow-serverless:ListTagsForResource",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource",
        "airflow-serverless:UpdateWorkflow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowCloudwatchLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:/aws/mwaa-serverless/${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}/*"
      ]
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
```

```
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless"
      ]
    },
    {
      "Sid" : "DataZoneUserPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GenerateCode",
        "datazone:CreateAsset*",
        "datazone:List*",
        "datazone:Search*",
        "datazone:*Message*",
        "datazone:*Conversation*",
        "datazone:*Cell*",
        "datazone:*Notebook*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaSession",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard",
        "athena:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBenchMLActionsWithResourceType",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sqlworkbench:GetConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioProjectUserRolePermissionsBoundary

Descrizione: Amazon SageMaker crea ruoli IAM per gli utenti di Projects per eseguire analisi dei dati, intelligenza artificiale e azioni di apprendimento automatico e utilizza questa politica durante la creazione di questi ruoli per definire i limiti delle loro autorizzazioni.

`SageMakerStudioProjectUserRolePermissionsBoundary`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioProjectUserRolePermissionsBoundary` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2024, 21:57 UTC

- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePermissionsBoundary`

Versione della politica

Versione della politica: v19 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAllNonMatchingProjectTag",
      "Effect" : "Deny",
      "Action" : "*",
      "NotResource" : [
        "arn:*:sagemaker:*:*:model-package-group/*",
        "arn:*:sagemaker:*:*:model-package/*",
        "arn:*:glue:*:*:catalog/*",
        "arn:*:glue:*:*:database/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AmazonQChatPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
```

```
            "ec2.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEmrEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "codecommit.*.amazonaws.com"
```

```
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants",
        "kms:GetPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "DataZoneDescribeKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaFederatedCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
 "arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessCertificateS3LocationPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "CloudWatchDescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:StartQuery",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:airflow*",
        "arn:aws:logs:*:*:log-group:datazone*"
      ]
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
```

```
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCrawlerPermissions",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetClassifier",
```

```
        "glue:GetClassifiers",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UseGlueStudio",
        "glue:ListSessions",
        "glue:StartCompletion",
        "glue:GetCompletion",
        "glue:GetGeneratedCode",
        "glue:GetTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GluePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:CancelStatement",
        "glue:ListStatements",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:DeleteSession",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:CancelDataQualityRuleRecommendationRun",
```

```
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:DeleteDataQualityRuleset",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:UpdateDataQualityRuleset"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "ec2.amazonaws.com",
            "emr-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsIAMSessionRestriction",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:GetQCustomContext",
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQSqlPromptQuotas",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAccessExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
```

```
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RedshifServerlessCredentialsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "redshift-data.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftExistingComputeConnectToCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "GenerativeAIPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:*-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "ManageNetworkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListImageVersions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListContexts",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListApps",
```

```
            "sagemaker:ListDomains",
            "sagemaker:ListUserProfiles",
            "sagemaker:ListSpaces",
            "sagemaker:ListTags",
            "sagemaker:DescribeMlflowTrackingServer",
            "sagemaker:DescribeImageVersion",
            "sagemaker:DescribeImage",
            "sagemaker:DescribeInferenceComponent",
            "sagemaker:DescribeEndpointConfig",
            "sagemaker:DescribeModel",
            "sagemaker:DescribeOptimizationJob",
            "sagemaker:DescribeEndpoint",
            "sagemaker:DescribeInferenceRecommendationsJob",
            "sagemaker:DescribeModelPackage",
            "sagemaker:DescribeModelPackageGroup",
            "sagemaker:DescribePipeline",
            "sagemaker:DescribePipelineExecution",
            "sagemaker:DescribePipelineDefinitionForExecution",
            "sagemaker:DescribeHyperParameterTuningJob",
            "sagemaker:DescribeAutoMLJob",
            "sagemaker:DescribeAutoMLJobV2",
            "sagemaker:DescribeProcessingJob",
            "sagemaker:DescribeTrainingJob",
            "sagemaker:DescribeAction",
            "sagemaker:DescribeArtifact",
            "sagemaker:DescribeTrialComponent",
            "sagemaker:DescribeContext",
            "sagemaker:DescribeDomain",
            "sagemaker:DescribeApp",
            "sagemaker:DescribeUserProfile",
            "sagemaker:DescribeSpace",
            "sagemaker:AddTags",
            "sagemaker:AddAssociation",
            "sagemaker:DeleteAssociation",
            "sagemaker:DeleteContext",
            "sagemaker:DeleteAction",
            "sagemaker:DeleteArtifact",
            "sagemaker:DeleteUserProfile",
            "sagemaker:UpdateSpace",
            "sagemaker:DeleteSpace",
            "sagemaker:DeleteApp",
            "sagemaker:CreatePresignedDomainUrl",
            "sagemaker:CreateUserProfile",
            "sagemaker:CreateSpace",
```

```
            "sagemaker:CreateApp",
            "sagemaker:CreateTrainingJob",
            "sagemaker:CreateTransformJob",
            "sagemaker:CreateProcessingJob",
            "sagemaker:CreateAutoMLJob",
            "sagemaker:CreateAutoMLJobV2",
            "sagemaker:CreateHyperParameterTuningJob",
            "sagemaker:CreateEndpointConfig",
            "sagemaker:CreateEndpoint",
            "sagemaker:CreateModel",
            "sagemaker:CreateModelPackage",
            "sagemaker:CreateModelPackageGroup",
            "sagemaker:CreatePipeline",
            "sagemaker:CreateContext",
            "sagemaker:CreateArtifact",
            "sagemaker:CreateAction",
            "sagemaker:CreateInferenceComponent",
            "sagemaker:UpdateInferenceComponentRuntimeConfig",
            "sagemaker:StopTrainingJob",
            "sagemaker:StopProcessingJob",
            "sagemaker:StopAutoMLJob",
            "sagemaker:StopHyperParameterTuningJob",
            "sagemaker:DescribeTransformJob",
            "sagemaker:StopTransformJob",
            "sagemaker:UpdateTrainingJob",
            "sagemaker:BatchGetMetrics",
            "sagemaker:BatchPutMetrics",
            "sagemaker:DeleteEndpointConfig",
            "sagemaker:DeleteEndpoint",
            "sagemaker:UpdateEndpoint",
            "sagemaker:UpdateEndpointWeightsAndCapacities",
            "sagemaker:BatchDescribeModelPackage",
            "sagemaker:UpdateModelPackage",
            "sagemaker:DeleteModel",
            "sagemaker:DeleteModelPackage",
            "sagemaker:DeleteModelPackageGroup",
            "sagemaker:DeleteTags",
            "sagemaker:DeleteInferenceComponent",
            "sagemaker:CreateInferenceRecommendationsJob",
            "sagemaker:InvokeEndpoint",
            "sagemaker:InvokeEndpointAsync",
            "sagemaker:InvokeEndpointWithResponseStream",
            "sagemaker:QueryLineage",
            "sagemaker:UpdatePipeline",
```

```
            "sagemaker:DeletePipeline",
            "sagemaker:UpdatePipelineExecution",
            "sagemaker:StartPipelineExecution",
            "sagemaker:StopPipelineExecution",
            "sagemaker:RetryPipelineExecution",
            "sagemaker:SendPipelineExecutionStepSuccess",
            "sagemaker:SendPipelineExecutionStepFailure",
            "sagemaker:GetSearchSuggestions",
            "sagemaker:Search",
            "sagemaker:UpdateMlflowTrackingServer",
            "sagemaker:StartMlflowTrackingServer",
            "sagemaker:StopMlflowTrackingServer",
            "sagemaker:CreatePresignedMlflowTrackingServerUrl",
            "sagemaker:ListPartnerApps",
            "sagemaker:CreatePartnerAppPresignedUrl",
            "sagemaker:DescribePartnerApp",
            "sagemaker:CallPartnerAppApi",
            "sagemaker-mlflow:AccessUI",
            "sagemaker-mlflow:CreateExperiment",
            "sagemaker-mlflow:SearchExperiments",
            "sagemaker-mlflow:GetExperiment",
            "sagemaker-mlflow:GetExperimentByName",
            "sagemaker-mlflow:DeleteExperiment",
            "sagemaker-mlflow:RestoreExperiment",
            "sagemaker-mlflow:UpdateExperiment",
            "sagemaker-mlflow:CreateRun",
            "sagemaker-mlflow:DeleteRun",
            "sagemaker-mlflow:RestoreRun",
            "sagemaker-mlflow:GetRun",
            "sagemaker-mlflow:LogMetric",
            "sagemaker-mlflow:LogBatch",
            "sagemaker-mlflow:LogModel",
            "sagemaker-mlflow:LogInputs",
            "sagemaker-mlflow:SetExperimentTag",
            "sagemaker-mlflow:SetTag",
            "sagemaker-mlflow:DeleteTag",
            "sagemaker-mlflow:LogParam",
            "sagemaker-mlflow:GetMetricHistory",
            "sagemaker-mlflow:SearchRuns",
            "sagemaker-mlflow:ListArtifacts",
            "sagemaker-mlflow:UpdateRun",
            "sagemaker-mlflow:CreateRegisteredModel",
            "sagemaker-mlflow:GetRegisteredModel",
            "sagemaker-mlflow:RenameRegisteredModel",
```

```
        "sagemaker-mlflow:UpdateRegisteredModel",
        "sagemaker-mlflow:DeleteRegisteredModel",
        "sagemaker-mlflow:GetLatestModelVersions",
        "sagemaker-mlflow:CreateModelVersion",
        "sagemaker-mlflow:GetModelVersion",
        "sagemaker-mlflow:UpdateModelVersion",
        "sagemaker-mlflow:DeleteModelVersion",
        "sagemaker-mlflow:SearchModelVersions",
        "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
        "sagemaker-mlflow:TransitionModelVersionStage",
        "sagemaker-mlflow:SearchRegisteredModels",
        "sagemaker-mlflow:SetRegisteredModelTag",
        "sagemaker-mlflow:DeleteRegisteredModelTag",
        "sagemaker-mlflow:DeleteModelVersionTag",
        "sagemaker-mlflow:DeleteRegisteredModelAlias",
        "sagemaker-mlflow:SetRegisteredModelAlias",
        "sagemaker-mlflow:GetModelVersionByAlias",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:DescribeImages",
        "elasticfilesystem:DescribeMountTargets",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ComputePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "sts:GetCallerIdentity",
        "sts:TagSession",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:TerminateJobFlows",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataLakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
```

```
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "EMRServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreatePlacementGroup",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeletePlacementGroup",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupGetPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupMutatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        }
      }
    },
    {
      "Sid" : "ModelRegistryBedRockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessAossCollectionsForBedrock",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*"
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:InvokeAgent",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases",
```

```
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateEvaluationJobForFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseDataIngestionKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "kms:ViaService" : "true",
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetDataZoneEnvironmentCfnStackPermissionsForBedrockAppExport",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "MWAAPermissions",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments",
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
    },
    {
      "Sid" : "SQSPermissionsForMWAA",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : "arn:aws:sqs:*:*:airflow-celery-*"
    },
    {
      "Sid" : "FederatedDataConnectionGlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueConnectionAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "GlueEntitiesAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretAccessForForUseWithAllDataZoneProjectsSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "AccessForDynamoDbConnections",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ListDomainS3BucketForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForAthenaCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-staging-bucket-*/*",
        "arn:aws:s3:::redshift-staging-bucket-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetS3ObjectForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*/dzd_*/*/dev/sys/athena/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "GetGlueUserDefinedFuncLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "airflow:CreateWebLoginToken",
        "airflow:GetEnvironment",
        "airflow:InvokeRestApi",
        "airflow:ListEnvironments",
        "airflow:UpdateEnvironment",
        "aoss:APIAccessAll",
```

```
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
```

```
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "bedrock:ApplyGuardrail",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateAgentAlias",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreatePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeletePrompt",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetEvaluationJob",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetPrompt",
        "bedrock:InvokeAgent",
        "bedrock:InvokeFlow",
        "bedrock:InvokeInlineAgent",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFoundationModels",
        "bedrock:ListIngestionJobs",
        "bedrock:ListPrompts",
```

```
            "bedrock:ListTagsForResource",
            "bedrock:Retrieve",
            "bedrock:RetrieveAndGenerate",
            "bedrock:StartIngestionJob",
            "bedrock:StopEvaluationJob",
            "bedrock:TagResource",
            "bedrock:UpdateAgentAlias",
            "cloudformation:DescribeStacks",
            "cloudformation:GetTemplate",
            "cloudwatch:DeleteAlarms",
            "cloudwatch:DescribeAlarms",
            "cloudwatch:GetMetricData",
            "cloudwatch:GetMetricStatistics",
            "cloudwatch:PutMetricAlarm",
            "cloudwatch:PutMetricData",
            "codecommit:BatchDescribeMergeConflicts",
            "codecommit:BatchGetCommits",
            "codecommit:BatchGetPullRequests",
            "codecommit:BatchGetRepositories",
            "codecommit:CreateBranch",
            "codecommit:CreateCommit",
            "codecommit:CreatePullRequest",
            "codecommit:DeleteBranch",
            "codecommit:DeleteFile",
            "codecommit:DescribeMergeConflicts",
            "codecommit:DescribePullRequestEvents",
            "codecommit:GetBlob",
            "codecommit:GetBranch",
            "codecommit:GetComment",
            "codecommit:GetCommentReactions",
            "codecommit:GetCommentsForComparedCommit",
            "codecommit:GetCommentsForPullRequest",
            "codecommit:GetCommit",
            "codecommit:GetCommitHistory",
            "codecommit:GetCommitsFromMergeBase",
            "codecommit:GetDifferences",
            "codecommit:GetFile",
            "codecommit:GetFolder",
            "codecommit:GetMergeCommit",
            "codecommit:GetMergeConflicts",
            "codecommit:GetMergeOptions",
            "codecommit:GetObjectIdentifier",
            "codecommit:GetPullRequest",
            "codecommit:GetPullRequestApprovalStates",
```

```
            "codecommit:GetPullRequestOverrideState",
            "codecommit:GetReferences",
            "codecommit:GetRepository",
            "codecommit:GetRepositoryTriggers",
            "codecommit:GetTree",
            "codecommit:GetUploadArchiveStatus",
            "codecommit:GitPull",
            "codecommit:GitPush",
            "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
            "codecommit:ListBranches",
            "codecommit:ListFileCommitHistory",
            "codecommit:ListPullRequests",
            "codecommit:ListTagsForResource",
            "codecommit:MergeBranchesByFastForward",
            "codecommit:MergeBranchesBySquash",
            "codecommit:MergeBranchesByThreeWay",
            "codecommit:MergePullRequestByFastForward",
            "codecommit:MergePullRequestBySquash",
            "codecommit:MergePullRequestByThreeWay",
            "codecommit:PostCommentForComparedCommit",
            "codecommit:PostCommentForPullRequest",
            "codecommit:PostCommentReply",
            "codecommit:PutCommentReaction",
            "codecommit:PutFile",
            "codecommit:UpdateComment",
            "codecommit:UpdateDefaultBranch",
            "codecommit:UpdatePullRequestApprovalRuleContent",
            "codecommit:UpdatePullRequestApprovalState",
            "codecommit:UpdatePullRequestDescription",
            "codecommit:UpdatePullRequestStatus",
            "codecommit:UpdatePullRequestTitle",
            "codecommit:UpdateRepositoryDescription",
            "codewhisperer:GenerateRecommendations",
            "datazone:CreateConnection",
            "datazone:DeleteConnection",
            "datazone:GetConnection",
            "datazone:GetDomain",
            "datazone:GetDomainExecutionRoleCredentials",
            "datazone:GetEnvironment",
            "datazone:GetEnvironmentBlueprintConfiguration",
            "datazone:GetProject",
            "datazone:GetUserProfile",
            "datazone:ListConnections",
            "datazone:ListEnvironmentBlueprints",
```

```
        "datazone:ListEnvironments",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeEndpoints",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeImport",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListImports",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "dynamodb:PutItem",
        "dynamodb:PartiQLSelect",
        "dynamodb:PartiQLInsert",
        "dynamodb:PartiQLUpdate",
        "dynamodb:PartiQLDelete",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateGlobalTable",
        "dynamodb:UpdateTable",
        "ec2:AttachNetworkInterface",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribePersistentAppUI",
```

```
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:TerminateJobFlows",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:CancelStatement",
        "glue:CreateBlueprint",
        "glue:CreateDatabase",
        "glue:CreateDataQualityRuleset",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateSession",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
```

```
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteDatabase",
        "glue:DeleteDataQualityRuleset",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteSession",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:DescribeConnectionType",
        "glue:DescribeEntity",
        "glue:GetCatalog",
        "glue:GetCatalogImportStatus",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetCompletion",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDashboardUrl",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:GetEntityRecords",
        "glue:GetGeneratedCode",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTables",
```

```
            "glue:GetTableVersion",
            "glue:GetTableVersions",
            "glue:GetTags",
            "glue:GetUserDefinedFunction",
            "glue:GetUserDefinedFunctions",
            "glue:ListConnectionTypes",
            "glue:ListCrawls",
            "glue:ListDataQualityResults",
            "glue:ListDataQualityRuleRecommendationRuns",
            "glue:ListDataQualityRulesetEvaluationRuns",
            "glue:ListDataQualityRulesets",
            "glue:ListEntities",
            "glue:ListSessions",
            "glue:ListStatements",
            "glue:ListTableOptimizerRuns",
            "glue:NotifyEvent",
            "glue:PassConnection",
            "glue:PublishDataQuality",
            "glue:PutDataQualityProfileAnnotation",
            "glue:PutDataQualityStatisticAnnotation",
            "glue:PutWorkflowRunProperties",
            "glue:ResumeWorkflowRun",
            "glue:RunStatement",
            "glue:SearchTables",
            "glue:StartBlueprintRun",
            "glue:StartCompletion",
            "glue:StartDataQualityRuleRecommendationRun",
            "glue:StartDataQualityRulesetEvaluationRun",
            "glue:StartJobRun",
            "glue:StartWorkflowRun",
            "glue:StopSession",
            "glue:StopWorkflowRun",
            "glue:TagResource",
            "glue:UntagResource",
            "glue:UpdateBlueprint",
            "glue:UpdateCatalog",
            "glue:UpdateColumnStatisticsForPartition",
            "glue:UpdateColumnStatisticsForTable",
            "glue:UpdateDataQualityRuleset",
            "glue:UpdateJob",
            "glue:UpdatePartition",
            "glue:UpdateTable",
            "glue:UpdateWorkflow",
            "glue:UseGlueStudio",
```

```
            "iam:CreateServiceLinkedRole",
            "iam:GetRole",
            "iam:ListRoles",
            "iam:PassRole",
            "kms:CreateGrant",
            "kms:Decrypt",
            "kms:DescribeKey",
            "kms:Encrypt",
            "kms:GenerateDataKey",
            "kms:GenerateDataKeyWithoutPlaintext",
            "kms:GetPublicKey",
            "kms:ListAliases",
            "kms:ListGrants",
            "kms:ReEncryptFrom",
            "kms:ReEncryptTo",
            "kms:RevokeGrant",
            "lakeformation:GetDataAccess",
            "lambda:InvokeFunction",
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams",
            "logs:FilterLogEvents",
            "logs:GetLogEvents",
            "logs:GetLogGroupFields",
            "logs:GetLogRecord",
            "logs:GetQueryResults",
            "logs:PutLogEvents",
            "logs:StartQuery",
            "logs:StopQuery",
            "pricing:GetProducts",
            "q:SendMessage",
            "q:StartConversation",
            "redshift-data:BatchExecuteStatement",
            "redshift-data:CancelStatement",
            "redshift-data:DescribeStatement",
            "redshift-data:DescribeTable",
            "redshift-data:ExecuteStatement",
            "redshift-data:GetStagingBucketLocation",
            "redshift-data:GetStatementResult",
            "redshift-data:ListDatabases",
            "redshift-data:ListSchemas",
            "redshift-data:ListStatements",
            "redshift-data:ListTables",
```

```
            "redshift-serverless:GetCredentials",
            "redshift-serverless:GetManagedWorkgroup",
            "redshift-serverless:GetNamespace",
            "redshift-serverless:GetWorkgroup",
            "redshift-serverless:ListNamespaces",
            "redshift-serverless:ListTagsForResource",
            "redshift-serverless:ListWorkgroups",
            "redshift:DescribeClusters",
            "redshift:DescribeTags",
            "redshift:GetClusterCredentialsWithIAM",
            "resource-groups:CreateGroup",
            "resource-groups:DeleteGroup",
            "resource-groups:GetGroupQuery",
            "resource-groups:ListGroupResources",
            "resource-groups:Tag",
            "s3:AbortMultipartUpload",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucketLocation",
            "s3:GetEncryptionConfiguration",
            "s3:GetObject*",
            "s3:ListBucket",
            "s3:ListBucketVersions",
            "s3:ListMultipartUploadParts",
            "s3:PutObject",
            "s3:PutObjectRetention",
            "s3:PutObjectTagging",
            "s3:ReplicateObject",
            "s3:RestoreObject",
            "sagemaker-mlflow:AccessUI",
            "sagemaker-mlflow:CreateExperiment",
            "sagemaker-mlflow:CreateModelVersion",
            "sagemaker-mlflow:CreateRegisteredModel",
            "sagemaker-mlflow:CreateRun",
            "sagemaker-mlflow:DeleteExperiment",
            "sagemaker-mlflow:DeleteModelVersion",
            "sagemaker-mlflow:DeleteModelVersionTag",
            "sagemaker-mlflow:DeleteRegisteredModel",
            "sagemaker-mlflow:DeleteRegisteredModelAlias",
            "sagemaker-mlflow:DeleteRegisteredModelTag",
            "sagemaker-mlflow:DeleteRun",
            "sagemaker-mlflow:DeleteTag",
            "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
```

```
            "sagemaker-mlflow:GetExperiment",
            "sagemaker-mlflow:GetExperimentByName",
            "sagemaker-mlflow:GetLatestModelVersions",
            "sagemaker-mlflow:GetMetricHistory",
            "sagemaker-mlflow:GetModelVersion",
            "sagemaker-mlflow:GetModelVersionByAlias",
            "sagemaker-mlflow:GetRegisteredModel",
            "sagemaker-mlflow:GetRun",
            "sagemaker-mlflow:ListArtifacts",
            "sagemaker-mlflow:LogBatch",
            "sagemaker-mlflow:LogInputs",
            "sagemaker-mlflow:LogMetric",
            "sagemaker-mlflow:LogModel",
            "sagemaker-mlflow:LogParam",
            "sagemaker-mlflow:RenameRegisteredModel",
            "sagemaker-mlflow:RestoreExperiment",
            "sagemaker-mlflow:RestoreRun",
            "sagemaker-mlflow:SearchExperiments",
            "sagemaker-mlflow:SearchModelVersions",
            "sagemaker-mlflow:SearchRegisteredModels",
            "sagemaker-mlflow:SearchRuns",
            "sagemaker-mlflow:SetExperimentTag",
            "sagemaker-mlflow:SetRegisteredModelAlias",
            "sagemaker-mlflow:SetRegisteredModelTag",
            "sagemaker-mlflow:SetTag",
            "sagemaker-mlflow:TransitionModelVersionStage",
            "sagemaker-mlflow:UpdateExperiment",
            "sagemaker-mlflow:UpdateModelVersion",
            "sagemaker-mlflow:UpdateRegisteredModel",
            "sagemaker-mlflow:UpdateRun",
            "sagemaker:AddAssociation",
            "sagemaker:AddTags",
            "sagemaker:BatchDescribeModelPackage",
            "sagemaker:BatchGetMetrics",
            "sagemaker:BatchPutMetrics",
            "sagemaker:CallPartnerAppApi",
            "sagemaker:CreateAction",
            "sagemaker:CreateApp",
            "sagemaker:CreateArtifact",
            "sagemaker:CreateAutoMLJob",
            "sagemaker:CreateAutoMLJobV2",
            "sagemaker:CreateContext",
            "sagemaker:CreateEndpoint",
            "sagemaker:CreateEndpointConfig",
```

```
            "sagemaker:CreateHyperParameterTuningJob",
            "sagemaker:CreateInferenceComponent",
            "sagemaker:CreateInferenceRecommendationsJob",
            "sagemaker:CreateModel",
            "sagemaker:CreateModelPackage",
            "sagemaker:CreateModelPackageGroup",
            "sagemaker:CreatePartnerAppPresignedUrl",
            "sagemaker:CreatePipeline",
            "sagemaker:CreatePresignedDomainUrl",
            "sagemaker:CreatePresignedMlflowTrackingServerUrl",
            "sagemaker:CreateProcessingJob",
            "sagemaker:CreateSpace",
            "sagemaker:CreateTrainingJob",
            "sagemaker:CreateTransformJob",
            "sagemaker:CreateUserProfile",
            "sagemaker:DeleteAction",
            "sagemaker:DeleteApp",
            "sagemaker:DeleteArtifact",
            "sagemaker:DeleteAssociation",
            "sagemaker:DeleteContext",
            "sagemaker:DeleteEndpoint",
            "sagemaker:DeleteEndpointConfig",
            "sagemaker:DeleteInferenceComponent",
            "sagemaker:DeleteModel",
            "sagemaker:DeleteModelPackage",
            "sagemaker:DeleteModelPackageGroup",
            "sagemaker:DeletePipeline",
            "sagemaker:DeleteSpace",
            "sagemaker:DeleteTags",
            "sagemaker:DeleteUserProfile",
            "sagemaker:DescribeAction",
            "sagemaker:DescribeApp",
            "sagemaker:DescribeArtifact",
            "sagemaker:DescribeAutoMLJob",
            "sagemaker:DescribeAutoMLJobV2",
            "sagemaker:DescribeContext",
            "sagemaker:DescribeDomain",
            "sagemaker:DescribeEndpoint",
            "sagemaker:DescribeEndpointConfig",
            "sagemaker:DescribeHyperParameterTuningJob",
            "sagemaker:DescribeImage",
            "sagemaker:DescribeImageVersion",
            "sagemaker:DescribeInferenceComponent",
            "sagemaker:DescribeInferenceRecommendationsJob",
```

```
            "sagemaker:DescribeMlflowTrackingServer",
            "sagemaker:DescribeModel",
            "sagemaker:DescribeModelPackage",
            "sagemaker:DescribeModelPackageGroup",
            "sagemaker:DescribeOptimizationJob",
            "sagemaker:DescribePartnerApp",
            "sagemaker:DescribePipeline",
            "sagemaker:DescribePipelineDefinitionForExecution",
            "sagemaker:DescribePipelineExecution",
            "sagemaker:DescribeProcessingJob",
            "sagemaker:DescribeSpace",
            "sagemaker:DescribeTrainingJob",
            "sagemaker:DescribeTransformJob",
            "sagemaker:DescribeTrialComponent",
            "sagemaker:DescribeUserProfile",
            "sagemaker:GetSearchSuggestions",
            "sagemaker:InvokeEndpoint",
            "sagemaker:InvokeEndpointAsync",
            "sagemaker:InvokeEndpointWithResponseStream",
            "sagemaker:ListApps",
            "sagemaker:ListArtifacts",
            "sagemaker:ListAssociations",
            "sagemaker:ListAutoMLJobs",
            "sagemaker:ListCandidatesForAutoMLJob",
            "sagemaker:ListContexts",
            "sagemaker:ListDomains",
            "sagemaker:ListEndpointConfigs",
            "sagemaker:ListEndpoints",
            "sagemaker:ListHubContents",
            "sagemaker:ListHubs",
            "sagemaker:ListHyperParameterTuningJobs",
            "sagemaker:ListImageVersions",
            "sagemaker:ListInferenceComponents",
            "sagemaker:ListMlflowTrackingServers",
            "sagemaker:ListModelMetadata",
            "sagemaker:ListModelPackageGroups",
            "sagemaker:ListModelPackages",
            "sagemaker:ListModels",
            "sagemaker:ListPartnerApps",
            "sagemaker:ListPipelineExecutions",
            "sagemaker:ListPipelineExecutionSteps",
            "sagemaker:ListPipelineParametersForExecution",
            "sagemaker:ListPipelines",
            "sagemaker:ListProcessingJobs",
```

```
            "sagemaker:ListSpaces",
            "sagemaker:ListTags",
            "sagemaker:ListTrainingJobs",
            "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
            "sagemaker:ListTransformJobs",
            "sagemaker:ListUserProfiles",
            "sagemaker:QueryLineage",
            "sagemaker:RetryPipelineExecution",
            "sagemaker:Search",
            "sagemaker:SendPipelineExecutionStepFailure",
            "sagemaker:SendPipelineExecutionStepSuccess",
            "sagemaker:StartMlflowTrackingServer",
            "sagemaker:StartPipelineExecution",
            "sagemaker:StopAutoMLJob",
            "sagemaker:StopHyperParameterTuningJob",
            "sagemaker:StopMlflowTrackingServer",
            "sagemaker:StopPipelineExecution",
            "sagemaker:StopProcessingJob",
            "sagemaker:StopTrainingJob",
            "sagemaker:StopTransformJob",
            "sagemaker:UpdateEndpoint",
            "sagemaker:UpdateEndpointWeightsAndCapacities",
            "sagemaker:UpdateInferenceComponentRuntimeConfig",
            "sagemaker:UpdateMlflowTrackingServer",
            "sagemaker:UpdateModelPackage",
            "sagemaker:UpdatePipeline",
            "sagemaker:UpdatePipelineExecution",
            "sagemaker:UpdateSpace",
            "sagemaker:UpdateTrainingJob",
            "secretsmanager:DescribeSecret",
            "secretsmanager:GetSecretValue",
            "secretsmanager:ListSecrets",
            "secretsmanager:PutSecretValue",
            "sqlworkbench:CreateConnection",
            "sqlworkbench:DeleteQCustomContext",
            "sqlworkbench:DeleteTab",
            "sqlworkbench:DriverExecute",
            "sqlworkbench:GetAutocompletionMetadata",
            "sqlworkbench:GetAutocompletionResource",
            "sqlworkbench:GetQCustomContext",
            "sqlworkbench:GetQSqlPromptQuotas",
            "sqlworkbench:GetQSqlRecommendations",
            "sqlworkbench:GetQueryExecutionHistory",
            "sqlworkbench:GetUserInfo",
```

```
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:ListTabs",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:PutTab",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "sts:AssumeRole",
        "sts:GetCallerIdentity",
        "sts:SetSourceIdentity",
        "sts:TagSession",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioProjectUserRolePolicy

Descrizione: Amazon SageMaker Studio crea ruoli IAM per consentire agli utenti dei progetti di eseguire azioni di analisi dei dati, intelligenza artificiale e apprendimento automatico e utilizza questa policy durante la creazione di questi ruoli per definire le autorizzazioni.

`SageMakerStudioProjectUserRolePolicy`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioProjectUserRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 20 novembre 2024, 21:59 UTC
- Ora modificata: 29 luglio 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy`

Versione della politica

Versione della politica: v73 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCommit",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
```

```
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
```

```
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CodeCommitKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CodeWhisperer",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGlueCreateEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "true"
        },
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueENIonSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueENIonSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws-glue-service-resource" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueEniOnInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeGlueEni",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKernelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
```

```
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueTagSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
```

```
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*Session*",
        "glue:*Statement*",
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:*DataQuality*",
```

```
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:BatchGetJobs",
        "glue:GetJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueDQ",
      "Effect" : "Allow",
      "Action" : "glue:ListDataQuality*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueDQVetl",
      "Effect" : "Allow",
      "Action" : [
        "glue:*DataQuality*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:dataQualityRuleset/dq_etl_ruleset_${aws:PrincipalTag/
AmazonDataZoneProject}_*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueListJobs",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListJobs"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueVisualETL",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetGeneratedCode"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCompletions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*",
        "arn:aws:glue:*:*:job/*"
      ]
    },
    {
      "Sid" : "GlueJobRunnerSessionLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws-glue/*"
    },
    {
      "Sid" : "EC2TagsForGlue",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/DefaultGlueCatalogKmsKeyId}",
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}"
      ],
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
```

```
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EMRS",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:*Session*",
        "emr-serverless:GetResourceDashboard",
        "emr-serverless:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowActionsForTaggedEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "AirflowListEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowUiApiAccess",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : [
        "arn:aws:airflow:*:*:role/DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}/User"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:airflow-DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}-*"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AmazonMWAA"
        }
      }
    },
    {
      "Sid" : "GlueJobCWPutMetricActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "Glue",
            "AWS/Glue",
            "Glue Data Quality"
          ]
        }
      }
    },
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowSqsActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
```

```
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:airflow-celery-*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountS3Permissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:GetPublicKey",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "XAcctKmsDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
```

```
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
 "arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "S3BucketAcl",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketAcl",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BREvalS3Tag",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
          ]
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "DomainS3BucketKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DZDomainKMSKeyXAcctPerm",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/DomainKmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:datazone:domainId" : "${aws:PrincipalTag/
AmazonDataZoneDomain}"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "ListLogGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueJobLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/*"
      ]
    },
    {
      "Sid" : "ProjectLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}:log-stream:*"
      ]
```

```
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
```

```
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AthenaDataCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:datacatalog/AwsDataCatalog",
        "arn:aws:athena:*:*:datacatalog/awsdatacatalog"
      ]
    },
    {
      "Sid" : "AthenaListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneUserPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "datazone:PostLineageEvent",
        "datazone:*Compute*"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/${aws:PrincipalTag/
AmazonDataZoneDomain}"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:UseConnection",
        "codestar-connections:GetConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "GlueGetDefaultDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowGlueGetDatabasesExceptDefault",
      "Effect" : "Allow",
      "Action" : "glue:GetDatabases",
      "NotResource" : "arn:aws:glue:*:*:database/default",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueListDatabasesOnNoDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueFileUploadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:UseGlueStudio"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueProjectConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnection",
        "glue:GetConnections"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueGetConnectionOnlyOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:DeleteDatabase",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
```

```
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "S3TCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*ColumnStatistics*",
        "glue:*Database*",
        "glue:*Partition*",
        "glue:*Table*",
        "glue:GetCatalog*",
        "glue:GetUserDefinedFunction*"
      ],
      "Resource" : "arn:*:glue:*:*:catalog/s3tablescatalog"
    },
    {
      "Sid" : "GlueCrawler",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "GlueGlobalTempDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueDefaultCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueNonDefaultCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "LFforDL",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess",
        "lakeformation:GetResourceLFTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "TagSessionForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "AmazonDataZoneDomain"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "${aws:PrincipalTag/
AmazonDataZoneDomain}",
```

```
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SetContextForTIP",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:sts::*:self"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "sqlworkbench.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "StsContext",
      "Effect" : "Allow",
      "Action" : "sts:SetContext",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        }
      }
    },
    {
      "Sid" : "GlueConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
```

```
        "glue:GetTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "UnrestrictedAccessGlueEntities",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntities",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleOnProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/RoleName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "airflow-serverless.amazonaws.com",
            "sagemaker.amazonaws.com",
            "glue.amazonaws.com",
            "airflow.amazonaws.com",
```

```
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "scheduler.amazonaws.com",
            "access-grants.s3.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletion*",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:*QCustomContext",
        "sqlworkbench:GetQSql*",
        "sqlworkbench:GetSchemaInference"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SQLWorkBenchActions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:AssociateNotebookWithTab",
      "Resource" : "arn:*:sqlworkbench:*:*:notebook/*"
    },
    {
      "Sid" : "SQLWorkBenchNotebookActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateNotebook*",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook*",
        "sqlworkbench:DeleteNotebook*",
        "sqlworkbench:ExportNotebook",
```

```
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RSDataIAMSession",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
```

```
        }
      }
    },
    {
      "Sid" : "ExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RSWgTagged",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RSExistCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeCredentials",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:*ManagedEndpoint*",
        "emr-containers:TagResource",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "redshift-serverless:GetCredentials",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RSDataMWg",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RssCreds",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "redshift-data.amazonaws.com",
            "sqlworkbench.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AllowTagGetResources",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGetSecretForRedShift",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "EMRClusterWithDataZoneTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:*Session*",
        "elasticmapreduce:AddTags"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRClusterInfoPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRGetClusterSessionCreds",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:GetClusterSessionCredentials"
```

```
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EmrContainersSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EMRPersistentAppUI",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:GetPersistentAppUIPresignedURL"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
```

```
    {
      "Sid" : "KmsWithEncrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "scheduler.*.amazonaws.com",
            "glue.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EBDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "emr-serverless.*.amazonaws.com",
            "redshift.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KmsManagement",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "scheduler.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsKeyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsManagement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2PermissionsForNotebookExecution",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeBRModel",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
```

```
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "bedrock:InferenceProfileArn" : "arn:aws:bedrock:*:*:application-inference-
profile/*"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModel",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
```

```
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BRInvokeAppProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AccessBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
```

```
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockResourceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ApplyGuardrail",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateAgentAlias",
        "bedrock:CreateBlueprint",
        "bedrock:CreateBlueprintVersion",
        "bedrock:CreateDataAutomationProject",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreatePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteBlueprint",
        "bedrock:DeleteDataAutomationProject",
        "bedrock:DeletePrompt",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentVersion",
        "bedrock:GetBlueprint",
```

```
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetEvaluationJob",
        "bedrock:GetIngestionJob",
        "bedrock:GetPrompt",
        "bedrock:InvokeAgent",
        "bedrock:InvokeDataAutomationAsync",
        "bedrock:InvokeFlow",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentVersions",
        "bedrock:ListIngestionJobs",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:StopEvaluationJob",
        "bedrock:UpdateAgentAlias",
        "bedrock:UpdateBlueprint",
        "bedrock:UpdateDataAutomationProject",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases"
      ],
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BREvalFM",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "BRCreateEval",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
```

```
      "Resource" : [
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*::foundation-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeDataAutomationAsyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeDataAutomationAsync"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:data-automation-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BedrockInvokeInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BRRAG",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockNoResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListEvaluationJobs",
        "bedrock:RetrieveAndGenerate",
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockTagResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonBedrockManaged",
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "BedrockKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KmsViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "kms:EncryptionContextKeys" : [
            "aws:bedrock*:arn",
            "aws:bedrock:guardrail-id"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "SecretPermissionsForBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerPermissionsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SecretKmsPermissionsForBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ArnLike" : {
```

```
          "kms:EncryptionContext:SecretARN" :
"arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BRKmsSM",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
"arn:aws:secretsmanager:*:*:secret:amazon-bedrock*"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "bedrock.amazonaws.com",
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "LambdaInvokeFunctionViaBedrock",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "bedrock.amazonaws.com",
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "DZEnvCfn",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CFNGetDataZoneEnvironmentStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLF",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueGetUserDefinedFunc",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataConnectionAllProjectResources",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "glue:GetConnections"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "DataConnectionLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/athenafederatedcatalog*"
    },
    {
      "Sid" : "DataConnOpen",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "glue:ManagedConnector",
        "glue:TestConnection",
        "codeconnections:GetHost",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:GetHost",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataConnectionEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
```

```
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "DataConnectionDeleteENI",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "DataConnectionDescribeENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:BatchDeleteImage",
        "ecr:ListTagsForResource",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:UploadLayerPart"
      ],
```

```
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateECRRepositoryPermission",
      "Effect" : "Allow",
      "Action" : "ecr:CreateRepository",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRTagResourcePermission",
      "Effect" : "Allow",
      "Action" : "ecr:TagResource",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRUntagResourcePermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "LFResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:DescribeResource",
        "ram:GetResourceShareInvitations",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:UpdateDataCellsFilter",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "XAcctLFCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Sid" : "XAcctRAMGlue",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "XAcctRAMLF",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        },
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Sid" : "RAMGetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "XAcctRAMInvite",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*",
            "DataZoneS3AG*"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "XAcctRAMLFHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule",
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "QSFolderDS",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:ListFolderMembers"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:folder/*",
        "arn:aws:quicksight:*:*:datasource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightOtherResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeUser",
        "quicksight:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ]
    },
    {
      "Sid" : "ManagePassDataSourcePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "quicksight:PassDataSource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageCreateDataSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:TagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateFolderMembership",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateFolderMembership"
      ],
```

```
      "Resource" : "arn:aws:quicksight:*:*:folder/sagemaker-*-assets",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneAssetsFolder" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioQueryExecutionRolePolicy

Descrizione: Amazon SageMaker Studio utilizza questa politica durante l'esecuzione di query su connessioni federate.

`SageMakerStudioQueryExecutionRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioQueryExecutionRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 31 gennaio 2025, 19:52 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioQueryExecutionRolePolicy`

Versione della politica

Versione della politica: v6 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueGetConnectionOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueGetConnectionsForProject",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "arn:aws:glue:*:*:connection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3GetObjectForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::*/dzd*/*/dev/sys/athena/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "S3ListBucketOwnershipCheckForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center

- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioUserIAMConsolePolicy

Descrizione: fornisce privilegi di configurazione individuali per Amazon SageMaker Unified Studio tramite l'SDK Console di gestione AWS and. Consente il lancio di Unified Studio Portal. SageMaker

`SageMakerStudioUserIAMConsolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioUserIAMConsolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2025, 22:49 UTC
- Ora modificata: 31 marzo 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMConsolePolicy`

Versione della politica

Versione della politica: v10 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "datazone:ListDomains",
        "datazone:GetDomain",
        "datazone:GetUserProfile",
        "datazone:ListProjects",
        "datazone:ListProjectProfiles",
        "datazone:CreateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:GetIamPortalLoginUrl",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironments",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetGroupProfile",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "datazone:ListProjectMemberships",
        "datazone:GetConnection",
        "datazone:ListConnections"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioUserIAMDefaultExecutionPolicy

Descrizione: politica di esecuzione per l'utilizzo dei ruoli IAM con SageMaker Unified Studio. Consente agli utenti di accedere alle risorse dell'account locale (escluso l'accesso alle risorse di dati) per IAM-based l'utilizzo di SageMaker Unified Studio.

`SageMakerStudioUserIAMDefaultExecutionPolicy`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioUserIAMDefaultExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2025, 17:19 UTC
- Ora modificata: 14 luglio 2026, 18:57 UTC

- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy`

Versione della politica

Versione della politica: v28 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
```

```
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:*Notebook*",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage",
        "datazone:CancelMessage",
        "datazone:QueryGraph",
        "datazone:StartCompute",
        "datazone:StopCompute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
```

```
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "Q",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
```

```
    },
    {
      "Sid" : "SageMakerUserTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerPrivateSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:CreateSpace",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "CanvasUserProfileApp",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp",
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/Canvas/*",
        "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Batch*",
        "sagemaker:Describe*",
        "sagemaker:List*",
```

```
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:*MlflowApp*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*",
        "sagemaker:*Feature*",
        "sagemaker:*Record"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model",
            "aws-jumpstart*",
            "Source",
            "CanvasModelName",
            "Canvas",
            "SageMaker",
            "ProjectS3Path",
            "Owner"
          ]
        },
```

```
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        }
      }
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:CreateCatalog",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:UseGlueStudio",
        "glue:*Resource",
        "glue:*Job*",
```

```
        "glue:TestConnection",
        "glue:*DataQuality*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
```

```
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/
AmazonDataZonePassedRolePath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "events.amazonaws.com",
            "pods.eks.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowMWAA",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccount",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:Get*",
        "scheduler:List*",
        "scheduler:UpdateSchedule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGet*",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
```

```
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:Get*",
        "athena:ImportNotebook",
        "athena:List*",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TagResource",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:UseConnection",
        "codestar-connections:GetConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsUserList",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetHost",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:GetHost",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
```

```
    {
      "Sid" : "AccessProjectS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject*",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject*",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/AmazonDataZoneProjectBucket}/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProjectBucket" : ""
        }
      }
    },
    {
      "Sid" : "EMR",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:Get*",
        "emr-serverless:List*",
        "emr-serverless:Start*",
        "emr-serverless:Access*Endpoints",
        "emr-serverless:Terminate*",
        "emr-serverless:*Resource",
        "emr-containers:*ManagedEndpoint*",
        "emr-containers:*SecurityConfiguration*",
        "emr-containers:*VirtualCluster*",
        "emr-containers:*Resource",
        "elasticmapreduce:*PersistentAppUI*",
        "elasticmapreduce:Start*",
        "elasticmapreduce:Get*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:Terminate*",
        "elasticmapreduce:*Tag*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CanvasGeneralPermissions",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:BatchDetect*",
        "comprehend:Detect*",
        "textract:Analyze*",
        "textract:Start*",
        "textract:Get*",
        "rekognition:Detect*",
        "sagemaker-data-science-assistant:*",
        "rds:DescribeDBInstances",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalingActivities",
        "quicksight:ListNamespaces",
        "events:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CanvasRedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "CanvasEventBridgePutOperation",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "CanvasEventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "CanvasEventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SageMakerStudioUserIAMPermissiveExecutionPolicy

Descrizione: politica di esecuzione per l'utilizzo dei ruoli IAM con SageMaker Unified Studio. Consente agli utenti di accedere alle risorse del tuo account (incluso un ampio accesso a tutte le API nei servizi di dati come S3, Glue, CloudWatch Logs e altri) per IAM-based l'utilizzo di SageMaker Unified Studio.

`SageMakerStudioUserIAMPermissiveExecutionPolicy`è una policy gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `SageMakerStudioUserIAMPermissiveExecutionPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 18 agosto 2025, 17:19 UTC
- Ora modificata: 14 luglio 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy`

Versione della politica

Versione della politica: v23 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*",
        "s3tables:*",
        "comprehend:*",
        "textract:*",
        "rekognition:*",
        "sagemaker-data-science-assistant:*",
        "rds:*",
        "quicksight:*",
        "events:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
        "elasticmapreduce:*",
        "emr-containers:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*",
        "airflow:*",
        "application-autoscaling:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
```

```
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
```

```
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
```

```
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:*Notebook*",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage",
        "datazone:CancelMessage",
        "datazone:QueryGraph",
        "datazone:StartCompute",
        "datazone:StopCompute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
```

```
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
```

```
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateSecret",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:UseConnection",
        "codestar-connections:GetConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsUserList",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetHost",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:GetHost",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
```

```
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SecretsManagerReadWrite

Descrizione: Fornisce read/write l'accesso a AWS Secrets Manager tramite Console di gestione AWS. Nota: questo esclude le azioni IAM, quindi combinalo con IAMFull Access se è richiesta la configurazione di rotazione.

`SecretsManagerReadWrite`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SecretsManagerReadWrite` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 4 aprile 2018, 18:05 UTC
- Ora modificata: 22 febbraio 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:*",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
```

```
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:SecretsManager*"
    },
    {
      "Sid" : "SARPermissions",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:CreateCloudFormationChangeSet",
        "serverlessrepo:GetApplication"
      ],
      "Resource" : "arn:aws:serverlessrepo:*:*:applications/SecretsManager*"
    },
    {
      "Sid" : "S3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo-changesets*",
        "arn:aws:s3:::secrets-manager-rotation-apps-*/*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SecurityAgentWebAppAPIPolicy

Descrizione: fornisce le autorizzazioni agli utenti autenticati per accedere all'applicazione Web Security Agent per la configurazione e l'esecuzione di test automatici di penetrazione della sicurezza. Questa politica consente agli utenti di gestire i pentest, visualizzare i risultati, monitorare l'esecuzione dei test e interagire con AWS le risorse necessarie per le operazioni di test di sicurezza.

`SecurityAgentWebAppAPIPolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SecurityAgentWebAppAPIPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 2 dicembre 2025, 15:04 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SecurityAgentWebAppAPIPolicy`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentInstances",
        "securityagent:ListControls"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentInstances",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetSecurityTestContentMetadata",
        "securityagent:BatchGetTasks",
        "securityagent:CreateDocumentReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
        "securityagent:DeleteDocumentReview",
        "securityagent:GetArtifact",
        "securityagent:GetCodeReviewTask",
        "securityagent:GetDocReviewTask",
        "securityagent:GetDocumentReview",
        "securityagent:GetDocumentReviewArtifact",
        "securityagent:ListArtifacts",
        "securityagent:ListControls",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDocumentReviewComments",
        "securityagent:ListDocumentReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListTasks",
```

```
        "securityagent:StartCodeRemediation",
        "securityagent:StartPentestExecution",
        "securityagent:StopPentestExecution",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-instance*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SecurityAgentWebAppPolicy

Descrizione: fornisce le autorizzazioni agli utenti autenticati per accedere all'applicazione Web Security Agent per la configurazione e l'esecuzione di test di penetrazione della sicurezza automatizzati. Questa politica consente agli utenti di gestire i pentest, visualizzare i risultati, monitorare l'esecuzione dei test e interagire con AWS le risorse necessarie per le operazioni di test di sicurezza.

`SecurityAgentWebAppPolicy`è una policy AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SecurityAgentWebAppPolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 05 febbraio 2026, 20:19 UTC
- Ora modificata: 12 febbraio 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAgentWebAppPolicy`

Versione della politica

Versione della politica: v3 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:ListSecurityRequirements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentSpaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
```

```
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobTasks",
        "securityagent:CreateDesignReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
        "securityagent:GetArtifact",
        "securityagent:DeleteDesignReview",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
        "securityagent:ListArtifacts",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListPentestJobTasks",
        "securityagent:StartCodeRemediation",
        "securityagent:StartPentestJob",
        "securityagent:StopPentestJob",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SecurityAudit

Descrizione: il modello di controllo di sicurezza consente l'accesso alla lettura dei metadati di configurazione di sicurezza. È utile per il software che verifica la configurazione di un. Account AWS

`SecurityAudit`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SecurityAudit` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 21 luglio 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Versione della politica

Versione della politica: v91 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseSecurityAuditStatement",
      "Effect" : "Allow",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
```

```
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appsync:GetApiCache",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
```

```
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentFrameworkShareRequests",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControlDomainInsights",
        "auditmanager:ListControlDomainInsightsByAssessment",
        "auditmanager:ListControlInsightsByControlDomain",
        "auditmanager:ListControls",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling:Describe*",
        "backup:DescribeGlobalSettings",
        "backup:DescribeRegionSettings",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupVaults",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetCustomModel",
        "bedrock:GetFlowAlias",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetImportedModel",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBaseDocuments",
        "bedrock:GetMarketplaceModelEndpoint",
        "bedrock:GetModelCopyJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelImportJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
```

```
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListImportedModels",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListMarketplaceModelEndpoints",
        "bedrock:ListModelCopyJobs",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelImportJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:ListTagsForResource",
        "bedrock-agentcore:GetABTest",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetBatchEvaluation",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetConfigurationBundleVersion",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetHarness",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPaymentInstrument",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPaymentSession",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetRecommendation",
        "bedrock-agentcore:GetRegistry",
```

```
        "bedrock-agentcore:GetRegistryRecord",
        "bedrock-agentcore:ListABTests",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimeVersions",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListBatchEvaluations",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListConfigurationBundleVersions",
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListHarnesses",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPaymentInstruments",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPaymentSessions",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyGenerationAssets",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListRecommendations",
        "bedrock-agentcore:ListRegistries",
        "bedrock-agentcore:ListRegistryRecords",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "chime:List*",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
```

```
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cloud9:Describe*",
        "cloud9:ListEnvironments",
        "clouddirectory:ListDirectories",
        "cloudformation:DescribeStack*",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStack*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomainEndpointOptions",
        "cloudsearch:DescribeDomains",
        "cloudsearch:DescribeServiceAccessPolicies",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
```

```
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetDashboard",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListTagsForResource",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListRepositories",
        "codebuild:BatchGetProjects",
        "codebuild:GetResourcePolicy",
        "codebuild:ListProjects",
        "codebuild:ListSourceCredentials",
        "codecommit:BatchGetRepositories",
        "codecommit:GetBranch",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:GetJobDetails",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "codestar:Describe*",
        "codestar:List*",
        "cognito-identity:Describe*",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:Describe*",
        "cognito-idp:ListDevices",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserImportJobs",
        "cognito-idp:ListUserPoolClients",
```

```
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "cognito-sync:Describe*",
        "cognito-sync:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "comprehendmedical:ListICD10CMInferenceJobs",
        "comprehendmedical:ListPHIDetectionJobs",
        "comprehendmedical:ListRxNormInferenceJobs",
        "comprehendmedical:ListSNOMEDCTInferenceJobs",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:ListApprovedOrigins",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListLexBots",
        "connect:ListSecurityKeys",
        "databrew:DescribeDataset",
        "databrew:DescribeProject",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "dataexchange:ListDataSets",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ValidatePipelineDefinition",
        "datasync:Describe*",
        "datasync:List*",
        "dax:Describe*",
        "dax:ListTags",
        "deepracer:ListModels",
```

```
        "detective:GetGraphIngestState",
        "detective:ListGraphs",
        "detective:ListMembers",
        "devicefarm:ListProjects",
        "directconnect:Describe*",
        "discovery:DescribeAgents",
        "discovery:DescribeConfigurations",
        "discovery:DescribeContinuousExports",
        "discovery:DescribeExportConfigurations",
        "discovery:DescribeExportTasks",
        "discovery:DescribeImportTasks",
        "dms:Describe*",
        "dms:ListTagsForResource",
        "docdb-elastic:ListClusters",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListBackups",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayPrefixListReferences",
```

```
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeAccessEntry",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "eks:ListAccessEntries",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodeGroups",
        "eks:ListTagsForResource",
        "eks:ListUpdates",
        "elasticache:Describe*",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
```

```
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elastictranscoder:ListPipelines",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdNamespace",
        "es:Describe*",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern",
        "finspace:ListEnvironments",
        "finspace:ListKxEnvironments",
        "firehose:Describe*",
        "firehose:List*",
        "fms:ListComplianceStatus",
        "fms:ListPolicies",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "geo:ListMaps",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetVaultAccessPolicy",
```

```
        "glacier:GetVaultLock",
        "glacier:ListVaults",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoints",
        "glue:GetJobs",
        "glue:GetResourcePolicy",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTags",
        "grafana:ListWorkspaces",
        "greengrass:List*",
        "guardduty:DescribeMalwareScans",
        "guardduty:DescribeOrganizationConfiguration",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
        "guardduty:List*",
        "health:DescribeAffectedAccountsForOrganization",
        "health:DescribeAffectedEntities",
        "health:DescribeAffectedEntitiesForOrganization",
        "health:DescribeEntityAggregates",
        "health:DescribeEventAggregates",
        "health:DescribeEventDetails",
        "health:DescribeEventDetailsForOrganization",
        "health:DescribeEvents",
        "health:DescribeEventsForOrganization",
        "health:DescribeEventTypes",
        "health:DescribeHealthServiceStatusForOrganization",
        "healthlake:ListFHIRDatastores",
        "honeycode:ListTables",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy",
        "identitystore:DescribeGroupMembership",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
```

```
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "iot:Describe*",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:List*",
        "iotanalytics:ListChannels",
        "iotevents:ListInputs",
        "iotfleetwise:ListModelManifests",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListWorkspaces",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
```

```
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeLimits",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListShards",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeEdgeConfiguration",
        "kinesisvideo:DescribeMappedResourceConfiguration",
        "kinesisvideo:DescribeMediaStorageConfiguration",
        "kinesisvideo:DescribeNotificationConfiguration",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:GetAccountSettings",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "lex:DescribeBot",
        "lex:DescribeResourcePolicy",
        "lex:ListBots",
        "license-manager:List*",
        "lightsail:GetBuckets",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancers",
```

```
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:ListDatasets",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:DescribeMLModels",
        "macie2:ListFindings",
        "managedblockchain:ListNetworks",
        "mechanicalturk:ListHITs",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:ListChannels",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListOriginEndpoints",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:ListContainers",
        "memorydb:DescribeClusters",
        "mq:DescribeBroker",
        "mq:DescribeBrokerEngineTypes",
        "mq:DescribeBrokerInstanceOptions",
        "mq:DescribeConfiguration",
        "mq:DescribeConfigurationRevision",
        "mq:DescribeUser",
        "mq:ListBrokers",
        "mq:ListConfigurationRevisions",
        "mq:ListConfigurations",
        "mq:ListTags",
        "mq:ListUsers",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
```

```
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "nimble:ListStudios",
        "opsworks-cm:DescribeServers",
        "opsworks:DescribeStacks",
        "organizations:Describe*",
        "organizations:List*",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDatasetGroup",
        "personalize:ListDatasetGroups",
        "private-networks:ListNetworks",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListDataSourceSyncJobs",
        "qbusiness:ListDocuments",
        "qbusiness:ListGroups",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:DownloadDBLogFilePortion",
```

```
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrantsInstanceResourcePolicy",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
```

```
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListCallerAccessGrants",
        "s3:ListJobs",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:ListAllMyDirectoryBuckets",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "s3tables:ListNamespaces",
```

```
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:GetVectors",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "s3vectors:ListVectors",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "sdb:DomainMetadata",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetCase",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:GetMembership",
        "security-ir:ListCaseEdits",
        "security-ir:ListCases",
        "security-ir:ListComments",
        "security-ir:ListInvestigations",
        "security-ir:ListMemberships",
```

```
        "security-ir:ListTagsForResource",
        "serverlessrepo:GetApplicationPolicy",
        "serverlessrepo:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:ListTagsForResource",
        "ses:Describe*",
        "ses:GetAccount",
        "ses:GetAccountSendingEnabled",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetIdentityDkimAttributes",
        "ses:GetIdentityPolicies",
        "ses:GetIdentityVerificationAttributes",
        "ses:ListConfigurationSets",
        "ses:ListDedicatedIpPools",
        "ses:ListIdentities",
        "ses:ListIdentityPolicies",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListVerifiedEmailAddresses",
        "shield:Describe*",
        "shield:GetSubscriptionState",
        "shield:List*",
        "snowball:ListClusters",
        "snowball:ListJobs",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
```

```
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:Describe*",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListAssociationVersions",
        "ssm:ListCommands",
        "ssm:ListComplianceItems",
        "ssm:ListComplianceSummaries",
        "ssm:ListDocumentMetadataHistory",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "ssm:ListInventoryEntries",
        "ssm:ListOpsMetadata",
        "ssm:ListResourceComplianceSummaries",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribeApplication",
        "sso:DescribeApplicationAssignment",
        "sso:DescribeApplicationProvider",
        "sso:DescribeInstance",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribeRegion",
        "sso:DescribeTrustedTokenIssuer",
        "sso:GetApplicationAccessScope",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:GetApplicationAuthenticationMethod",
        "sso:GetApplicationGrant",
        "sso:GetApplicationSessionConfiguration",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListAccountAssignmentCreationStatus",
        "sso:ListAccountAssignmentDeletionStatus",
        "sso:ListAccountAssignments",
        "sso:ListAccountAssignmentsForPrincipal",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListApplicationAccessScopes",
        "sso:ListApplicationAssignments",
```

```
        "sso:ListApplicationAssignmentsForPrincipal",
        "sso:ListApplicationAuthenticationMethods",
        "sso:ListApplicationGrants",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationInstances",
        "sso:ListApplicationProviders",
        "sso:ListApplications",
        "sso:ListApplicationTemplates",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListDirectoryAssociations",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetProvisioningStatus",
        "sso:ListPermissionSets",
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListRegions",
        "sso:ListTagsForResource",
        "sso:ListTrustedTokenIssuers",
        "sso-directory:ListExternalIdPConfigurationsForDirectory",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "storagegateway:DescribeBandwidthRateLimit",
        "storagegateway:DescribeCache",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:DescribeMaintenanceStartTime",
        "storagegateway:DescribeNFSFileShares",
        "storagegateway:DescribeSnapshotSchedule",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:DescribeTapeArchives",
        "storagegateway:DescribeTapeRecoveryPoints",
        "storagegateway:DescribeTapes",
        "storagegateway:DescribeUploadBuffer",
        "storagegateway:DescribeVTLDevices",
        "storagegateway:DescribeWorkingStorage",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "synthetics:DescribeCanaries",
```

```
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "tag:GetTagKeys",
        "transcribe:GetCallAnalyticsCategory",
        "transcribe:GetMedicalVocabulary",
        "transcribe:GetVocabulary",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsCategories",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListLanguageModels",
        "transcribe:ListMedicalTranscriptionJobs",
        "transcribe:ListMedicalVocabularies",
        "transcribe:ListTagsForResource",
        "transcribe:ListTranscriptionJobs",
        "transcribe:ListVocabularies",
        "transcribe:ListVocabularyFilters",
        "transfer:Describe*",
        "transfer:List*",
        "translate:List*",
        "trustedadvisor:Describe*",
        "voiceid:DescribeDomain",
        "waf-regional:GetWebACL",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:ListTagsForResource",
        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
```

```
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "wisdom:GetAssistant",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
```

```
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SecurityLakeResourceManagementServiceRolePolicy

Descrizione: fornisce l'accesso alla gestione delle risorse create da Security Lake.

`SecurityLakeResourceManagementServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 novembre 2024, 22:10 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeResourceManagementServiceRolePolicy`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "ManageSecurityLakeEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AmazonSecurityLake-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeLambdaConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:PutFunctionConcurrency",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetRuntimeManagementConfig",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:PublishVersion",
        "lambda:DeleteFunctionConcurrency",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetAlias",
        "lambda:GetPolicy",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeletePartitionUpdaterLambda",
      "Effect" : "Allow",
```

```
      "Action" : "lambda:DeleteFunction",
      "Resource" :
"arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListLambdaEventSourceMappings",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaEventSourceMapping",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateEventSourceMapping"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "lambda:FunctionArn" :
"arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaConfigs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateFunctionConfiguration"
```

```
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:GetTables",
        "glue:UpdateTable",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeConfigurationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObjectAttributes",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:GetReplicationConfiguration"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCompactionAndManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadSecurityLakeLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetQueryResults",
        "logs:GetLogRecord"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeSQSQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:StartMessageMoveTask",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ChangeMessageVisibility",
        "sqs:ListMessageMoveTasks",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake_*",
        "arn:aws:sqs:*:*:AmazonSecurityLakeManager-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SecurityLakeServiceLinkedRole

Descrizione: questa politica concede le autorizzazioni per gestire il servizio Amazon Security Lake per tuo conto

`SecurityLakeServiceLinkedRole`è una policy AWS gestita.

Utilizzo di questa politica

Questa politica è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica di ruolo Service-linked
- Ora di creazione: 29 novembre 2022, 14:03 UTC
- Ora modificata: 15 luglio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Versione della politica

Versione della politica: v4 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeOrgAccounts",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*"
      ]
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
    },
    {
      "Sid" : "AllowListServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationTrailValidation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAnyVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowWafLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "wafv2:LogScope" : "SecurityLake"
        }
      }
```

```
    },
    {
      "Sid" : "AllowPutLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
        }
      }
    },
    {
      "Sid" : "ListWebACLs",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListWebACLs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ServerMigration_ServiceRole

Descrizione: Autorizzazioni per consentire al AWS Server Migration Service di migrare le VM verso EC2: consente al Server Migration Service di collocare le risorse migrate nell'account EC2 del cliente.

`ServerMigration_ServiceRole`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `ServerMigration_ServiceRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 11 agosto 2020, 20:41 UTC
- Ora modificata: 15 ottobre 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ServerMigrationConnector

Descrizione: Autorizzazioni per consentire al AWS Server Migration Connector di migrare le macchine virtuali su EC2. Consente la comunicazione con il AWS Server Migration Service, read/write l'accesso ai bucket S3 che iniziano con 'sms-b-' e 'import-to-ec2-', nonché ai bucket utilizzati per l'aggiornamento del Server Migration Connector, la registrazione del AWS Server Migration Connector con e il caricamento delle metriche AWS su. AWS AWS

`ServerMigrationConnector`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `ServerMigrationConnector` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 ottobre 2016, 21:45 UTC
- Ora modificata: 24 ottobre 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:SendMessage",
        "sms:GetMessages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::sms-b-*",
        "arn:aws:s3:::import-to-ec2-*",
        "arn:aws:s3:::server-migration-service-upgrade",
        "arn:aws:s3:::server-migration-service-upgrade/*",
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "awsconnector:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ServerMigrationServiceConsoleFullAccess

Descrizione: autorizzazioni necessarie per utilizzare tutte le funzionalità della Server Migration Service Console

`ServerMigrationServiceConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ServerMigrationServiceConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 09 maggio 2020, 17:18 UTC
- Ora modificata: 20 luglio 2020, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sms:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "s3:ListAllMyBuckets",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sms.amazonaws.com"
        }
      },
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ServerMigrationServiceLaunchRole

Descrizione: Autorizzazioni per consentire al Servizio di migrazione dei AWS server di creare e aggiornare AWS le risorse pertinenti presso il cliente Account AWS per l'avvio di server e applicazioni migrati.

`ServerMigrationServiceLaunchRole`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `ServerMigrationServiceLaunchRole` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 26 novembre 2018, 19:53 UTC
- Ora modificata: 15 ottobre 2020, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ServerMigrationServiceRoleForInstanceValidation

Descrizione: autorizzazioni per consentire all' AWS SMS di eseguire lo script di convalida dei dati utilizzato e di inviare lo script success/failure a SMS

`ServerMigrationServiceRoleForInstanceValidation`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ServerMigrationServiceRoleForInstanceValidation` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 20 luglio 2020, 22:25 UTC
- Ora modificata: 20 luglio 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ServiceQuotasFullAccess

Descrizione: Fornisce l'accesso completo a Service Quotas

`ServiceQuotasFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ServiceQuotasFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2019, 15:44 UTC
- Ora modificata: 04 febbraio 2021, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
```

```
        "tag:GetTagValues",
        "servicequotas:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/ServiceQuotaMonitor" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "servicequotas.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ServiceQuotasReadOnlyAccess

Descrizione: Fornisce l'accesso in sola lettura a Service Quotas

`ServiceQuotasReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `ServiceQuotasReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 24 giugno 2019, 15:31 UTC
- Ora modificata: 12 febbraio 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Versione della politica

Versione della politica: v5 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServices",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListTagsForResource",
        "servicequotas:GetAutoManagementConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:GetNotificationConfiguration",
        "notifications:GetEventRule",
        "notifications:ListNotificationHubs",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:GetEmailContact",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
```

```
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackChannelConfigurations",
        "consoleapp:ListDeviceIdentities",
        "consoleapp:GetDeviceIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ServiceQuotasServiceRolePolicy

Descrizione: consente a Service Quotas di creare casi di assistenza per conto dell'utente

`ServiceQuotasServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 22 maggio 2019, 20:44 UTC
- Ora modificata: 24 giugno 2019, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SignInLocalDevelopmentAccess

Descrizione: fornisce le autorizzazioni per l'accesso programmatico AWS tramite il AWS servizio di accesso, inclusa la creazione di OAuth2 token per strumenti e applicazioni di sviluppo.

`SignInLocalDevelopmentAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `SignInLocalDevelopmentAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 19 novembre 2025, 18:34 UTC
- Ora modificata: 12 febbraio 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/SignInLocalDevelopmentAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "signin:AuthorizeOAuth2Access",
        "signin:CreateOAuth2Token"
      ],
      "Resource" : "arn:aws:signin:*:*:oauth2/public-client/*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SimpleWorkflowFullAccess

Descrizione: fornisce l'accesso completo al servizio di configurazione Simple Workflow.

`SimpleWorkflowFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SimpleWorkflowFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 6 febbraio 2015, 18:41 UTC
- Ora modificata: 6 febbraio 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SMSVoiceServiceRolePolicy

Descrizione: consente SMSVoice di pubblicare metriche per tuo CloudWatch conto

`SMSVoiceServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 14 novembre 2024, 17:04 UTC
- Ora modificata: 14 novembre 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SMSVoiceServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SMSVoice"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SplitCostAllocationDataServiceRolePolicy

Descrizione: consente ai dati di allocazione dei costi suddivisi di recuperare le informazioni di AWS Organizations, se applicabile, e raccogliere dati di telemetria per i servizi di dati di allocazione dei costi suddivisi per i quali il cliente ha scelto di aderire.

`SplitCostAllocationDataServiceRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 16 aprile 2024, 16:05 UTC
- Ora modificata: 16 aprile 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonManagedServiceForPrometheusAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:ListWorkspaces",
        "aps:QueryMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SSMQuickSetupRolePolicy

Descrizione: fornisce le autorizzazioni per verificare lo stato della configurazione di Quick Setup, garantire un uso coerente dei parametri e delle risorse assegnate e correggere le risorse quando viene rilevata una deriva.

`SSMQuickSetupRolePolicy`è una politica gestita.AWS

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: politica relativa ai ruoli collegati al servizio
- Ora di creazione: 25 giugno 2024, 15:20 UTC
- Ora modificata: 18 novembre 2024, 13:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SSMQuickSetupRolePolicy`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMResourceDataSyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SSMResourceDataSyncGetOpsSummaryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
    },
    {
      "Sid" : "SSMResourceDataSyncManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*",
      "Condition" : {
        "StringEquals" : {
          "ssm:SyncType" : "SyncFromSource"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListAssociations",
        "ssm:DescribeAssociationExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupSSMDocumentsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*",
        "arn:aws:ssm:*:*:document/*-AWSQuickSetupType-*"
      ]
    },
    {
```

```
      "Sid" : "OrganizationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedServicesForAccount"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupStackSetReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*"
      ]
    },
    {
      "Sid" : "QuickSetupStackSetDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*",
```

```
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset-target/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuickSetupCfnStacksDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SupportUser

Descrizione: questo criterio concede le autorizzazioni per la risoluzione dei problemi e la risoluzione di problemi in un. Account AWS Questa politica consente inoltre all'utente di contattare l' AWS assistenza per creare e gestire i casi.

`SupportUser`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SupportUser` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:21 UTC
- Ora modificata: 12 febbraio 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Versione della politica

Versione della politica: v11 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
```

```
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudtrail:ListTags",
        "cloudtrail:ListPublicKeys",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codecommit:BatchGetRepositories",
        "codecommit:Get*",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:AcknowledgeJob",
        "codepipeline:AcknowledgeThirdPartyJob",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:PollForJobs",
        "codepipeline:PollForThirdPartyJobs",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipeline",
        "cognito-identity:List*",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:Describe*",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:GetBulkPublishDetails",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:GetIdentityPoolConfiguration",
        "cognito-sync:List*",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetResourceConfigHistory",
        "config:ListDiscoveredResources",
        "datapipeline:DescribeObjects",
```

```
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ReportTaskProgress",
        "datapipeline:ReportTaskRunnerHeartbeat",
        "devicefarm:List*",
        "devicefarm:Get*",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:ListConfigurations",
        "dms:Describe*",
        "dms:List*",
        "ds:DescribeDirectories",
        "ds:DescribeSnapshots",
        "ds:GetDirectoryLimits",
        "ds:GetSnapshotLimits",
        "ds:ListAuthorizedApplications",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:Describe*",
        "ec2:DescribeHosts",
        "ec2:describeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeNatGateways",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeTags",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:GetRepositoryPolicy",
        "ecr:BatchCheckLayerAvailability",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticbeanstalk:ValidateConfigurationSettings",
```

```
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "elastictranscoder:ReadJob",
        "elasticfilesystem:DescribeFileSystems",
        "es:Describe*",
        "es:List*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "events:DescribeRule",
        "events:List*",
        "events:TestEventPattern",
        "firehose:Describe*",
        "firehose:List*",
        "gamelift:List*",
        "gamelift:Describe*",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:DescribeJob",
        "glacier:Get*",
        "glacier:List*",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "importexport:GetStatus",
        "importexport:ListJobs",
        "inspector:Describe*",
        "inspector:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:DiscoverInputSchema",
        "kinesisanalytics:GetApplicationState",
        "kinesisanalytics:ListApplications",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
```

```
        "lambda:List*",
        "lambda:Get*",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "opsworks:Describe*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "redshift:Describe*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:CheckDomainAvailability",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:List*",
        "s3:List*",
        "sdb:GetAttributes",
        "sdb:List*",
        "sdb:Select*",
        "servicecatalog:SearchProducts",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ScanProvisionedProducts",
        "ses:Get*",
        "ses:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
```

```
        "sqs:ReceiveMessage",
        "ssm:List*",
        "ssm:Describe*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "waf:Get*",
        "waf:List*",
        "workdocs:Describe*",
        "workmail:Describe*",
        "workmail:Get*",
        "workspaces:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

SystemAdministrator

Descrizione: concede le autorizzazioni di accesso complete necessarie per le risorse necessarie per le operazioni di applicazione e sviluppo.

`SystemAdministrator`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `SystemAdministrator` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:23 UTC
- Ora modificata: 12 febbraio 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Versione della politica

Versione della politica: v12 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
```

```
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
        "ec2:Allocate*",
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
        "ec2:Copy*",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateFlowLogs",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreatePlacementGroup",
        "ec2:CreateReservedInstancesListing",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateSpotDatafeedSubscription",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
```

```
        "ec2:CreateVpnGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteKeyPair",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSpotDatafeedSubscription",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DeregisterImage",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVolumeIO",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetConsoleOutput",
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetLaunchTemplateData",
        "ec2:GetPasswordData",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:Import*",
        "ec2:Modify*",
        "ec2:MonitorInstances",
        "ec2:MoveAddressToVpc",
        "ec2:Purchase*",
        "ec2:RegisterImage",
        "ec2:Release*",
        "ec2:Replace*",
        "ec2:ReportInstanceStatus",
        "ec2:Request*",
```

```
        "ec2:Reset*",
        "ec2:RestoreAddressToClassic",
        "ec2:RunScheduledInstances",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnmonitorInstances",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticloadbalancing:*",
        "events:*",
        "iam:GetAccount*",
        "iam:GetContextKeys*",
        "iam:GetCredentialReport",
        "iam:ListAccountAliases",
        "iam:ListGroups",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:Simulate*",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:List*",
        "lambda:PublishVersion",
        "lambda:Update*",
        "logs:*",
        "rds:Describe*",
        "rds:ListTagsForResource",
```

```
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:PutNotificationSettings",
        "rolesanywhere:ResetNotificationSettings",
        "route53:*",
        "route53domains:*",
        "ses:*",
        "sns:*",
        "sqs:*",
        "trustedadvisor:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl*",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachVolume",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RebootInstances",
```

```
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "s3:*",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetAccessKeyLastUsed",
        "iam:GetGroup*",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy*",
        "iam:GetRole*",
        "iam:GetSAMLProvider",
        "iam:GetSSHPublicKey",
        "iam:GetServerCertificate",
        "iam:GetServiceLastAccessed*",
        "iam:GetUser*",
        "iam:ListAccessKeys",
        "iam:ListAttached*",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles*",
        "iam:ListMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListSSHPublicKeys",
```

```
        "iam:ListSigningCertificates",
        "iam:ListUserPolicies",
        "iam:Upload*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/ec2-sysadmin-*",
        "arn:aws:iam::*:role/ecr-sysadmin-*",
        "arn:aws:iam::*:role/lambda-sysadmin-*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

TranslateFullAccess

Descrizione: fornisce l'accesso completo ad Amazon Translate.

`TranslateFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `TranslateFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 27 novembre 2018, 23:36 UTC
- Ora modificata: 08 gennaio 2020, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "translate:*",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

TranslateReadOnly

Descrizione: fornisce accesso in sola lettura ad Amazon Translate.

`TranslateReadOnly`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `TranslateReadOnly` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2017, 18:22 UTC
- Ora modificata: 24 maggio 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Versione della politica

Versione della politica: v7 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "translate:TranslateText",
        "translate:TranslateDocument",
        "translate:GetTerminology",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:ListParallelData",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

ViewOnlyAccess

Descrizione: questa politica concede le autorizzazioni per visualizzare risorse e metadati di base in tutti i servizi. AWS

`ViewOnlyAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `ViewOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: Job function policy
- Ora di creazione: 10 novembre 2016, 17:20 UTC
- Ora modificata: 22 aprile 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Versione della politica

Versione della politica: v45 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationGroup",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "backup:DescribeBackupJob",
        "backup:DescribeBackupVault",
        "backup:DescribeCopyJob",
        "backup:DescribeFramework",
        "backup:DescribeGlobalSettings",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
```

```
        "backup:DescribeRegionSettings",
        "backup:DescribeReportJob",
        "backup:DescribeReportPlan",
        "backup:DescribeRestoreJob",
        "backup:GetSupportedResourceTypes",
        "backup:ListBackupJobs",
        "backup:ListBackupPlans",
        "backup:ListBackupPlanTemplates",
        "backup:ListBackupPlanVersions",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListCopyJobs",
        "backup:ListFrameworks",
        "backup:ListLegalHolds",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByLegalHold",
        "backup:ListRecoveryPointsByResource",
        "backup:ListReportJobs",
        "backup:ListReportPlans",
        "backup:ListRestoreJobs",
        "backup:ListTags",
        "batch:ListJobs",
        "bedrock:ListCustomModels",
        "bedrock:ListTagsForResource",
        "clouddirectory:ListAppliedSchemaArns",
        "clouddirectory:ListDevelopmentSchemaArns",
        "clouddirectory:ListDirectories",
        "clouddirectory:ListPublishedSchemaArns",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomains",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codebuild:ListBuilds*",
        "codebuild:ListProjects",
        "codecommit:List*",
        "codedeploy:BatchGetApplicationRevisions",
```

```
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeploymentInstances",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:BatchGetOnPremisesInstances",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:ListPipelines",
        "codestar:List*",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:List*",
        "cognito-sync:ListDatasets",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:List*",
        "connect:List*",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetAccountLimits",
        "datapipeline:ListPipelines",
        "dax:DescribeClusters",
        "dax:DescribeDefaultParameters",
        "dax:DescribeEvents",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "devicefarm:List*",
        "directconnect:Describe*",
        "discovery:List*",
        "dms:List*",
        "ds:DescribeDirectories",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
```

```
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHost*",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeImage*",
        "ec2:DescribeImport*",
        "ec2:DescribeInstance*",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetwork*",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
```

```
        "ec2:DescribeReserved*",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshot*",
        "ec2:DescribeSpot*",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolume*",
        "ec2:DescribeVpc*",
        "ec2:DescribeVpnGateways",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeAddonConfiguration",
        "eks:DescribeAddonVersions",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeClusterVersions",
        "eks:DescribeEksAnywhereSubscription",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeInsight",
        "eks:DescribeInsightsRefresh",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:DescribeUpdate",
        "eks:ListAccessEntries",
        "eks:ListAccessPolicies",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListInsights",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
```

```
        "eks:ListTagsForResource",
        "eks:ListUpdates",
        "elasticache:Describe*",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListAvailableSolutionStacks",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "emr-serverless:ListApplications",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:ListDomainNames",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fsx:DescribeFileSystems",
        "gamelift:List*",
        "glacier:List*",
        "glue:GetTags",
        "greengrass:List*",
        "iam:GetAccountSummary",
        "iam:GetLoginProfile",
        "iam:List*",
        "importexport:ListJobs",
        "inspector:List*",
        "iot:List*",
        "kafka:ListClusters",
        "kendra:ListDataSources",
        "kendra:ListTagsForResource",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kms:ListKeys",
        "kms:ListResourceTags",
```

```
        "lambda:List*",
        "lex:GetBotAliases",
        "lex:GetBotChannelAssociations",
        "lex:GetBots",
        "lex:GetBotVersions",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetRegions",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered",
        "logs:Describe*",
        "logs:GetTransformer",
        "logs:ListEntitiesForLogGroup",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetImportJobs",
        "mobiletargeting:GetSegments",
```

```
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "opsworks-cm:Describe*",
        "opsworks:Describe*",
        "organizations:List*",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites",
        "outposts:ListTagsForResource",
        "polly:Describe*",
        "polly:List*",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "rds:Describe*",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEvents",
        "redshift:ViewQueriesInConsole",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
```

```
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sdb:List*",
        "servicecatalog:List*",
        "ses:DescribeActiveReceiptRuleSet",
        "ses:List*",
        "ses:ListDedicatedIpPools",
        "shield:List*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "states:ListActivities",
        "states:ListExecutions",
        "states:ListMapRuns",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "storagegateway:ListGateways",
        "storagegateway:ListLocalDisks",
        "storagegateway:ListVolumeRecoveryPoints",
        "storagegateway:ListVolumes",
        "swf:List*",
        "trustedadvisor:Describe*",
        "uxc:GetAccountCustomizations",
        "uxc:ListServices",
        "waf-regional:List*",
        "waf:List*",
        "wafv2:List*",
        "workdocs:DescribeAvailableDirectories",
        "workdocs:DescribeInstances",
        "workmail:Describe*",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroups",
        "xray:GetSamplingRules",
```

```
        "xray:GetSamplingStatisticSummaries",
        "xray:GetSamplingTargets",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
```

```
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

VMImportExportRoleForAWSConnector

Descrizione: policy predefinita per il ruolo di Import/Export servizio VM, per i clienti che utilizzano il AWS Connector. Il Import/Export servizio VM assume un ruolo con questa politica per soddisfare le richieste di migrazione delle macchine virtuali dall'appliance virtuale AWS Connector. (Si noti che il AWS Connector utilizza la politica gestita AWSConnector "" per inviare richieste per conto del cliente al servizio Import/Export VM.) Offre la possibilità di creare AMI e snapshot EBS, modificare gli attributi delle snapshot EBS, effettuare chiamate «Describe*» su oggetti EC2 e leggere dai bucket S3 che iniziano con '2-'. import-to-ec

`VMImportExportRoleForAWSConnector`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `VMImportExportRoleForAWSConnector` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica del ruolo di servizio
- Ora di creazione: 3 settembre 2015, 20:48 UTC
- Ora modificata: 3 settembre 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

VPCLatticeFullAccess

Descrizione: fornisce l'accesso completo ad Amazon VPC Lattice e l'accesso ai servizi di dipendenza.

`VPCLatticeFullAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `VPCLatticeFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 marzo 2023, 02:49 UTC
- Ora modificata: 12 febbraio 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "logs:DescribeLogGroups",
        "s3:ListAllMyBuckets",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

VPCLatticeReadOnlyAccess

Descrizione: fornisce accesso in sola lettura ad Amazon VPC Lattice tramite i servizi di dipendenza e accesso limitato ai Console di gestione AWS servizi di dipendenza.

`VPCLatticeReadOnlyAccess`è una politica gestita.AWS

Utilizzo di questa politica

È possibile associare la policy `VPCLatticeReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 marzo 2023, 02:47 UTC
- Ora modificata: 12 febbraio 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "logs:DescribeLogGroups",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "s3:ListAllMyBuckets",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

VPCLatticeServicesInvokeAccess

Descrizione: fornisce l'accesso per richiamare i servizi Amazon VPC Lattice.

`VPCLatticeServicesInvokeAccess`è una politica gestita AWS .

Utilizzo di questa politica

È possibile associare la policy `VPCLatticeServicesInvokeAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 30 marzo 2023, 02:45 UTC
- Ora modificata: 30 marzo 2023, 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

WAFLoggingServiceRolePolicy

Descrizione: creazione di una SLR per scrivere i log dei clienti in un flusso Firehose

`WAFLoggingServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 24 agosto 2018, 21:05 UTC
- Ora modificata: 20 maggio 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

WAFRegionalLoggingServiceRolePolicy

Descrizione: creazione di una SLR per scrivere i log dei clienti in un flusso Firehose

`WAFRegionalLoggingServiceRolePolicy`è una politica gestita AWS .

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 24 agosto 2018, 18:40 UTC
- Ora modificata: 20 maggio 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

WAFV2LoggingServiceRolePolicy

Descrizione: questa policy crea un ruolo collegato al servizio che consente a AWS WAF di scrivere log su Amazon Kinesis Data Firehose.

`WAFV2LoggingServiceRolePolicy`AWS è una politica gestita.

Utilizzo di questa politica

Questa policy è associata a un ruolo collegato al servizio che consente al servizio di eseguire azioni per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Dettagli della policy

- Tipo: Service-linked politica del ruolo
- Ora di creazione: 07 novembre 2019, 00:40 UTC
- Ora modificata: 20 maggio 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Versione della politica

Versione della politica: v4 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FirehoseAPIStatement",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "DescribeOrganizationAPIStatement",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Ulteriori informazioni

- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

WellArchitectedAgentResourceScanning

Descrizione: concede all' AWS Well-Architected agente l'accesso in sola lettura alle configurazioni AWS delle risorse, alle impostazioni di sicurezza e ai dati operativi per generare consigli di ottimizzazione

`WellArchitectedAgentResourceScanning`è una policy gestita. AWS

Utilizzo di questa politica

È possibile associare la policy `WellArchitectedAgentResourceScanning` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 16 luglio 2026, 20:27 UTC
- Ora modificata: 16 luglio 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedAgentResourceScanning`

Versione della politica

Versione della politica: v1 (impostazione predefinita)

La versione predefinita della policy è la versione che definisce le autorizzazioni per la policy. Quando un utente o un ruolo con la policy effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della policy per determinare se consentire la richiesta.

Documento sulla politica JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudControlDiscoveryCompact",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "aco-automation:GetAutomationRule",
        "aco-automation:ListAutomationRules",
        "aidevops:DescribePrivateConnection",
        "aidevops:Get*",
        "aidevops:List*",
        "aiops:Get*",
        "aiops:List*",
        "airflow-serverless:GetWorkflow",
        "airflow-serverless:List*",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "amplify:Get*",
        "amplify:List*",
        "amplifyuibuilder:Get*",
        "amplifyuibuilder:List*",
        "apigateway:GetRoutingRule",
        "apigateway:ListRoutingRules",
        "app-integrations:Get*",
        "app-integrations:List*",
        "appconfig:Get*",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
```

```
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "apptest:GetTestCase",
        "apptest:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-region-switch:GetPlan",
        "arc-region-switch:List*",
        "arc-zonal-shift:Get*",
        "arc-zonal-shift:ListManagedResources",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "aws-external-anthropic:GetWorkspace",
        "aws-external-anthropic:List*",
        "b2bi:Get*",
        "b2bi:List*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:List*",
        "bcm-pricing-calculator:GetBillScenario",
        "bcm-pricing-calculator:List*",
        "bedrock-agentcore:Get*",
        "bedrock-agentcore:List*",
        "bedrock-mantle:GetProject",
        "bedrock-mantle:List*",
        "bedrock:Get*",
        "bedrock:List*",
        "billing:GetBillingView",
        "billing:List*",
        "billingconductor:List*",
        "braket:ListTagsForResource",
        "braket:Search*",
        "budgets:Describe*",
```

```
        "budgets:ListTagsForResource",
        "ce:DescribeCostCategoryDefinition",
        "ce:Get*",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:List*",
        "chime:Describe*",
        "chime:List*",
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*",
        "cleanrooms:Get*",
        "cleanrooms:List*",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListTypes",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudwatch:Describe*",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:Get*",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricWidgetImage",
        "cloudwatch:List*",
        "cloudwatch:ListMetrics",
        "codeartifact:Describe*",
        "codeartifact:Get*",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:ListFleets",
        "codecommit:Get*",
        "codeconnections:GetConnection",
        "codeconnections:List*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codeguru-profiler:DescribeProfilingGroup",
```

```
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:Get*",
        "codestar-connections:List*",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:ListNotificationRules",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:Get*",
        "cognito-identity:ListIdentityPools",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "connect-campaigns:Describe*",
        "connect-campaigns:List*",
        "controltower:Get*",
        "controltower:List*",
        "cur:Describe*",
        "cur:ListTagsForResource",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:Get*",
        "deadline:List*",
        "detective:Describe*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:Get*",
        "devops-guru:List*",
        "directconnect:Describe*",
        "dms:Describe*",
        "dms:List*",
```

```
        "ds:Describe*",
        "ds:ListTagsForResource",
        "dsql:Get*",
        "dsql:List*",
        "ecr-public:Describe*",
        "ecr-public:Get*",
        "ecr-public:ListTagsForResource",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:List*",
        "elemental-inference:GetFeed",
        "elemental-inference:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "entityresolution:Get*",
        "entityresolution:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetSegment",
        "evidently:List*",
        "evs:GetEnvironment",
        "evs:List*",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fis:Get*",
        "fis:List*",
        "fms:Get*",
        "fms:List*",
        "forecast:Describe*",
```

```
        "forecast:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:Get*",
        "gameliftstreams:List*",
        "geo:Describe*",
        "geo:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "grafana:Describe*",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:Get*",
        "groundstation:List*",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
        "guardduty:List*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:List*",
        "iam:Get*",
        "iam:List*",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "inspector:Describe*",
        "inspector:List*",
        "inspector2:Get*",
        "inspector2:List*",
        "interconnect:GetConnection",
        "interconnect:List*",
        "internetmonitor:Get*",
        "internetmonitor:List*",
        "invoicing:GetInvoiceUnit",
        "invoicing:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
```

```
        "iotevents:Describe*",
        "iotevents:List*",
        "iotfleetwise:Get*",
        "iotfleetwise:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iottwinmaker:Get*",
        "iottwinmaker:List*",
        "iotwireless:Get*",
        "iotwireless:List*",
        "ivs:Get*",
        "ivs:List*",
        "ivschat:Get*",
        "ivschat:List*",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:Get*",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:List*",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:List*",
        "lambda:GetFunctionConcurrency",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "lex:Describe*",
        "lex:GetBotAlias",
        "lex:List*",
        "license-manager:Get*",
        "license-manager:List*",
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
```

```
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:Get*",
        "m2:List*",
        "macie2:Get*",
        "macie2:List*",
        "managedblockchain:GetAccessor",
        "managedblockchain:ListAccessors",
        "mediaconnect:Describe*",
        "mediaconnect:Get*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:Get*",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:Get*",
        "mediapackagev2:List*",
        "mediatailor:Describe*",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:List*",
        "medical-imaging:GetDatastore",
        "medical-imaging:List*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "mpa:Get*",
        "mpa:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:Get*",
        "networkmanager:List*",
        "nimble:GetStudio",
        "nimble:ListStudios",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:List*",
        "notifications:Get*",
        "notifications:List*",
```

```
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:Get*",
        "oam:List*",
        "observabilityadmin:Get*",
        "observabilityadmin:List*",
        "odb:Get*",
        "odb:List*",
        "omics:Get*",
        "omics:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:Get*",
        "osis:List*",
        "panorama:Describe*",
        "panorama:List*",
        "payment-cryptography:Get*",
        "payment-cryptography:List*",
        "pca-connector-ad:Get*",
        "pca-connector-ad:List*",
        "pca-connector-scep:Get*",
        "pca-connector-scep:List*",
        "pcs:Get*",
        "pcs:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:Get*",
        "profile:List*",
        "proton:Get*",
        "proton:List*",
        "qbusiness:Get*",
        "qbusiness:List*",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:List*",
        "refactor-spaces:Get*",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
```

```
        "resiliencehub:Describe*",
        "resiliencehub:Get*",
        "resiliencehub:List*",
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "robomaker:Describe*",
        "robomaker:List*",
        "rolesanywhere:Get*",
        "rolesanywhere:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53profiles:Get*",
        "route53profiles:List*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rtbfabric:Get*",
        "rtbfabric:List*",
        "rum:BatchGetRumMetricDefinitions",
        "rum:Get*",
        "rum:List*",
        "sagemaker:Describe*",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:List*",
        "sagemaker:ListMonitoringSchedules",
        "scheduler:Get*",
        "scheduler:List*",
        "schemas:Describe*",
        "schemas:List*",
        "securitylake:Get*",
        "securitylake:List*",
        "servicecatalog:Describe*",
        "servicecatalog:Get*",
        "servicecatalog:List*",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
```

```
        "signer:Get*",
        "signer:List*",
        "simspaceweaver:DescribeSimulation",
        "simspaceweaver:ListSimulations",
        "sms-voice:Describe*",
        "sms-voice:Get*",
        "sms-voice:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:List*",
        "ssm-contacts:Get*",
        "ssm-contacts:List*",
        "ssm-guiconnect:Get*",
        "ssm-incidents:Get*",
        "ssm-incidents:List*",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "states:Describe*",
        "states:List*",
        "supportapp:Get*",
        "supportapp:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:GetResources",
        "thinclient:GetEnvironment",
        "thinclient:List*",
        "transfer:Describe*",
        "transfer:List*",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListRecommendationResources",
        "trustedadvisor:ListRecommendations",
        "trustedadvisor:ListRecommendationsForResource",
        "verifiedpermissions:Get*",
        "verifiedpermissions:List*",
        "voiceid:DescribeDomain",
        "voiceid:List*",
```

```
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "wafv2:Get*",
        "wafv2:List*",
        "wisdom:Get*",
        "wisdom:List*",
        "workspaces-instances:Get*",
        "workspaces-instances:List*",
        "workspaces-web:Get*",
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:Get*",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudControlDiscoveryCompactExact",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "appsync:GetApi",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
```

```
        "appsync:ListDomainNames",
        "appsync:ListFunctions",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "cases:BatchGetCaseRule",
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudformation:ListTypeVersions",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "connect:DescribeAgentStatus",
        "connect:DescribeContactFlow",
```

```
        "connect:DescribeContactFlowModule",
        "connect:DescribeContactFlowModuleAlias",
        "connect:DescribeDataTable",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribeNotification",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeView",
        "connect:DescribeWorkspace",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListBots",
        "connect:ListContactFlowModuleAliases",
        "connect:ListContactFlowModules",
        "connect:ListContactFlowModuleVersions",
        "connect:ListContactFlows",
        "connect:ListContactFlowVersions",
        "connect:ListDataTableAttributes",
        "connect:ListDataTables",
        "connect:ListEvaluationForms",
        "connect:ListEvaluationFormVersions",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListNotifications",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
```

```
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUserProficiencies",
        "connect:ListUsers",
        "connect:ListViews",
        "connect:ListViewVersions",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchWorkspaceAssociations",
        "datazone:GetDataSource",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetProject",
        "datazone:GetProjectProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListDataSources",
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
```

```
        "datazone:ListEnvironments",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjectProfiles",
        "datazone:ListProjects",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeCapacityManagerDataExports",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHosts",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceSqlHaStates",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamPrefixListResolvers",
        "ec2:DescribeIpamPrefixListResolverTargets",
        "ec2:DescribeIpamResourceDiscoveries",
```

```
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpams",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilterRules",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:DescribeVerifiedAccessInstances",
```

```
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointAssociations",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConcentrators",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetIpamPrefixListResolverRules",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMeteringPolicyEntries",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
```

```
        "es:GetApplication",
        "es:ListApplications",
        "es:ListTags",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "glue:DescribeIntegrations",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetCrawler",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetIntegrationResourceProperty",
        "glue:GetJob",
        "glue:GetRegistry",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetUsageProfile",
        "glue:ListCrawlers",
        "glue:ListIntegrationResourceProperties",
        "glue:ListJobs",
        "glue:ListRegistries",
        "glue:ListSchemas",
        "glue:ListSchemaVersions",
        "glue:ListTriggers",
        "glue:ListUsageProfiles",
        "identitystore:DescribeGroup",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "kms:DescribeCustomKeyStores",
```

```
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:GetParametersForImport",
        "kms:GetPublicKey",
        "kms:ListAliases",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeyRotations",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "kms:ListRetirableGrants",
        "lambda:GetAlias",
        "lambda:GetCapacityProvider",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
```

```
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "neptune-graph:GetGraph",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListGraphs",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:ListTagsForResource",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListTagsForResource",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
```

```
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListTagsForResource",
```

```
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
```

```
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetInventoryConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
```

```
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
        "s3vectors:ListVectorBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListAgentSpaces",
        "securityagent:ListApplications",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetSecurityControls",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeSecurityHubV2",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetConnectorV2",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:GetInsights",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRules",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListConnectorsV2",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
```

```
        "securityhub:ListOrganizationAdminAccounts",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeDocument",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetMaintenanceWindowTask",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso-directory:DescribeGroup",
        "sso-directory:SearchGroups",
        "sts:GetCallerIdentity",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeScheduledQuery",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListScheduledQueries",
        "timestream:ListTables",
        "timestream:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando politiche AWS gestite in IAM Identity Center
- Aggiungere e rimuovere le autorizzazioni di identità IAM
- Comprendi il controllo delle versioni per le policy IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

WellArchitectedConsoleFullAccess

Descrizione: fornisce l'accesso completo allo AWS Well-Architected strumento tramite Console di gestione AWS

`WellArchitectedConsoleFullAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `WellArchitectedConsoleFullAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 29 novembre 2018, 18:19 UTC
- Ora modificata: 09 luglio 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Versione della politica

Versione della politica: v2 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wellarchitected:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "agent.wellarchitected.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:List*",
        "trustedadvisor:Get*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:*:iam::*:role/aws-service-role/*/
AWSServiceRoleForWellArchitected*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "wellarchitected.amazonaws.com",
            "agent.wellarchitected.amazonaws.com",
            "metrics.wellarchitected.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/*/
AWSServiceRoleForWellArchitected*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/service-role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "wellarchitected.amazonaws.com",
            "agent.wellarchitected.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

WellArchitectedConsoleReadOnlyAccess

Descrizione: fornisce l'accesso in sola lettura allo AWS Well-Architected strumento tramite Console di gestione AWS

`WellArchitectedConsoleReadOnlyAccess`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `WellArchitectedConsoleReadOnlyAccess` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita

- Ora di creazione: 29 novembre 2018, 18:21 UTC
- Ora modificata: 09 luglio 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Versione della politica

Versione della politica: v3 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "trustedadvisor:List*",
        "trustedadvisor:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

WorkLinkServiceRolePolicy

Descrizione: consente l'accesso Servizi AWS e le risorse utilizzate o gestite da Amazon WorkLink

`WorkLinkServiceRolePolicy`è una politica AWS gestita.

Utilizzo di questa politica

È possibile associare la policy `WorkLinkServiceRolePolicy` a utenti, gruppi e ruoli.

Dettagli della policy

- Tipo: politica AWS gestita
- Ora di creazione: 23 gennaio 2019, 19:03 UTC
- Ora modificata: 23 gennaio 2019, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Versione della politica

Versione della politica: v1 (predefinita)

La versione predefinita della politica è la versione che definisce le autorizzazioni per la politica. Quando un utente o un ruolo con la politica effettua una richiesta di accesso a una AWS risorsa, AWS controlla la versione predefinita della politica per determinare se consentire la richiesta.

Documento di policy JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonWorkLink-*"
    }
  ]
}
```

Ulteriori informazioni

- Crea un set di autorizzazioni utilizzando le policy AWS gestite in IAM Identity Center
- Aggiungere e rimuovere i permessi di identità IAM
- Comprendi il controllo delle versioni per le politiche IAM
- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.